ATLANTIS LAND

WebShare RB300

Wireless N Broadband Router

A02-RB-W300N

MANUALE COMPLETO

A02-RB-W300N _MI01

Where solutions begin

ISO 9001:2000 Company certified

INDICE

A02-RB-W300N_MI01 (V1.0 Maggio 2008)

AVVERTENZE

Abbiamo fatto di tutto al fine di evitare che nel testo, nelle immagini e nelle tabelle presenti in questo manuale, nel software e nell'hardware fossero presenti degli errori. Tuttavia, non possiamo garantire che non siano presenti errori e/o omissioni. Infine, non possiamo essere ritenuti responsabili per qualsiasi perdita, danno o incomprensione compiuti direttamente o indirettamente, come risulta dall'utilizzo del manuale, software e/o hardware.

Il contenuto di questo manuale è fornito esclusivamente per uso informale, è soggetto a cambiamenti senza preavviso (a tal fine si invita a consultare il sito www.atlantisland.it o www.atlantis-land.com per reperirne gli aggiornamenti) e non deve essere interpretato come un impegno da parte di Atlantis Land spa che non si assume responsabilità per qualsiasi errore o inesattezza che possa apparire in questo manuale. Nessuna parte di questa pubblicazione può essere riprodotta o trasmessa in altra forma o con qualsiasi mezzo, elettronicamente o meccanicamente, comprese fotocopie, riproduzioni, o registrazioni in un sistema di salvataggio, oppure tradotti in altra lingua e in altra forma senza un espresso permesso scritto da parte di Atlantis Land spa. Tutti i nomi di produttori e dei prodotti e qualsiasi marchio, registrato o meno, menzionati in questo manuale sono usati al solo scopo identificativo e rimangono proprietà esclusiva dei loro rispettivi proprietari.

Restrizioni di responsabilità CE/EMC

Il prodotto descritto in questa guida è stato progettato, prodotto e approvato in conformità alle regole EMC ed è stato certificato per non avere limitazioni EMC.

Se il prodotto fosse utilizzato con un PC non certificato, il produttore non garantisce il rispetto dei limiti EMC. Il prodotto descritto è stato costruito, prodotto e certificato in modo che i valori misurati rientrino nelle limitazioni EMC. In pratica, ed in particolari circostanze, potrebbe essere possibile che detti limiti possano essere superati se utilizzato con apparecchiature non prodotte nel rispetto della certificazione EMC. Può anche essere possibile, in alcuni casi, che i picchi di valore siano al di fuori delle tolleranze. In questo caso l’utilizzatore è responsabile della “compliance” con i limiti EMC. Il Produttore non è da ritenersi responsabile nel caso il prodotto sia utilizzato al di fuori delle limitazioni EMC.

CE Mark Warning

Questo dispositivo appartiene alla classe B. In un ambiente domestico il dispositivo può causare interferenze radio, in questo caso è opportuno prendere le adeguate contromisure.

ATTENZIONE

Lasciare almeno 30cm di distanza tra le antenne del dispositivo e l’utilizzatore.

Contrassegno CE
Questo dispositivo è stato testato ed è risultato conforme alla direttiva 1999/5/CE (2003/03/09) del parlamento Europeo e della Commissione Europea, a proposito di apparecchiature radio e periferiche per telecomunicazioni e loro mutuo riconoscimento. Dopo l'installazione, la periferica è stata trovata conforme ai seguenti standard: EN 300.328(radio), EN 301 489-17(compatibilità elettromagnetica), EN 60950-1 (sicurezza), EN55022 e EN55024. Questa apparecchiatura può pertanto essere utilizzata in tutti i paesi della Comunità Economica Europea ed in tutti i paesi dove viene applicata la Direttiva 1999/5/CE, senza restrizioni eccezion fatta per:
Francia:
Se si utilizza all'aperto tale dispositivo, la potenza in uscita è limitata (potenza e frequenza) in base alla tabella allegata. Per informazioni ulteriori consultare **www.art-telecom.fr.**

Luogo	Banda di Frequenze(MHz)	Potenza (EIRP)
Chiuso (senza restrizioni)	2400-2483,5	100mW(20dBm)
Aperto	2400-2454 2454-2483,5	100mW(20dBm) 10mW(10dBm)

Se l'uso di questa apparecchiatura in ambienti domestichi genera interferenze, è obbligo dell'utente porre rimedio a tale situazione.
Italia:
Questa periferica è conforme con l'Interfaccia Radio Nazionale e rispetta i requisiti sull'Assegnazione delle Frequenze. L'utilizzo di questa apparecchiatura al di fuori di ambienti in cui opera il proprietario, richiede un'autorizzazione generale. Per ulteriori informazioni si prega di consultare: **www.comunicazioni.it.**

La dichiarazione di conformità CE completa può essere reperita all'indirizzo web: www.atlantis-land.com nella pagina del prodotto.

CAPITOLO 1: Introduzione

Questo manuale è stato pensato per un utilizzo avanzato Wireless Broadband Router, per questo sono stati trattati con dovizia di particolari una moltitudine di argomenti che potrebbero, almeno inizialmente, scoraggiare alcuni utenti.
Per una configurazione rapida è comunque disponibile una Guida all'Installazione presente sia su CDRom che su supporto cartaceo a corredo del prodotto.

1.1 Panoramica di prodotto

Grazie per aver scelto WebShare RB300, la soluzione Atlantis Land per rendere la vostra rete senza fili veloce, scattante ed finalmente adatta ad applicazioni impegnative quali HD streaming e gaming online.
Semplice da installare, veloce e flessibile, il prodotto è in grado di offrire una piena mobilità attraverso un accesso wireless e, grazie al pieno supporto dei precedenti standard IEEE 802.11b/g, permette un aggiornamento graduale della rete preesistente, senza l'obbligo della sostituzione dei client già esistenti.
La tecnologia radio MIMO (Multiple-Input-Multiple-Output) e le 3 antenne (di cui 2 esterne, orientabili e rimovibili) permettono un importante incremento sia in termini di throughput (fino a 14 volte) che in termini di copertura (fino a 10 volte) rispetto agli standard precedenti, ed il chipset Atheros è in grado di garantire il pieno supporto hardware degli standard di sicurezza più recenti come il Wi-Fi Protected Access (WPA/WPA2) ed IEEE 802.11i, senza nessuna degradazione in termini di performance.
Le 5 porte Fast Ethernet, in grado di negoziare in maniera automatica sia la velocità di trasmissione (10/100, Half/Full-Duplex) che il tipo di cavo utilizzato (dritto o incrociato), permettono la creazione di una rete domestica senza la necessità della stesura di un cablaggio dedicato e la tecnologia OneTouch Configuration (conforme alle più recenti specifiche Wi-Fi Protected SetupTM),unita al Wizard Setup, permettono la configurazione della rete in piena autonomia anche per l'utenza meno esperta.
Il sofisticato firewall integrato (con funzionalità avanzate di ispezione dei pacchetti, anti intrusione, URL Blocking e Domain Blocking) renderà la vostra rete wireless a prova di hackers e grazie al client Dynamic DNS integrato, il prodotto può essere raggiunto e configurato anche da remoto, indipendentemente dal tipo di abbonamento ADSL utilizzato.

1.2 Contenuto della confezione

Una volta aperta la confezione, dovrebbero essere presenti i seguenti componenti:

- Wireless Broadband Router
- CDRom contenente manuale e QSG

- Guida di Quick Start (Italiano e Inglese)
- Alimentatore AC-DC (5V DC@2.5A)
- 2 Antenna da 2.2 dBi rimovibili (R-SMA Connector)
- Tagliando di garanzia

Qualora mancasse uno qualsiasi di questi componenti rivolgersi immediatamente al rivenditore.

1.3 Caratteristiche tecniche

Caratteristiche offerte dal Wireless Broadband Router:

- **Conforme alle specifiche 802.11n:** Grazie alla conformità con le più recenti specifiche 802.11n, il prodotto è in grado di offrire importanti icrementi sia in termini di velocità (fino a 300 Mbps*) che in termini di copertura (fino a 10 volte più ampia).
- **Piena compatibilità con gli standard IEEE 802.11g** e **IEEE 802.11b**: E' possibile utilizzare tutti gli apparati esistenti compatibili col protocollo IEEE802.11g e/o IEEE802.11b.
- **Funzionalità Wi-Fi Protected Access (WPA/WPA2) e WEP encryption**: E' possibile utilizzare il massimo livello di sicurezza senza nessuna degradazione di performance.
- **3 Antenne:** Due antenne esterne sostituibili ed orientabili ed una ed una interna fissa per sfruttare al meglio la tecnologia di trasmissione MIMO (Multiple-Input-Multiple-Output).
- **5 porte Fast Ethernet:** tutte e 5 le porte integrano la funzionalità MDI-II/MDI-X e pertanto possono funzionare indipendentemente tanto con cavi dritti che incrociati. Grazie a questa funzionalità è sufficiente collegare i dispositivi, penserà il dispositivo ad adeguarsi al tipo di cavo.
- **Quick Installation Wizard:** Grazie al supporto di un'interfaccia di configurazione via WEB, l'apparato risulta essere facilmente configurabile. E' disponibile inoltre una comodissima Wizard che guida passo passo l'utente alla configurazione del Router.
- **Network Address Translation (NAT):** Consente a diversi utenti di accedere alle risorse esterne, come Internet, simultaneamente attraverso un indirizzo IP singolo. Sono inoltre supportate direttamente : ICQ, FTP, Telnet, E-mail, News, Net2phone, Ping, NetMeeting e altro.
- **Firewall:** Supporta un SOHO firewall con tecnologia NAT. Automaticamente scopre e blocca l'attacco di tipo Denial of Service (DoS) attack. Il Wireless Broadband Router è fornito anche di un filtro di tipo URL Blocking e Domain Blocking per una maggiore profondità di filtraggio dei pericoli derivanti da Internet. L'attacco dell'hacker è registrato e conservato in un'area protetta.

- **Dynamic Domain Name System (DDNS):** Il Client Dynamic DNS permette di associare ad un indirizzo IP dinamico (che vi viene di volta in volta assegnato dal server dell'ISP) un nome statico (host-name). E' necessario, per utilizzare il sevizio, effettuare una registrazione gratuita per esempio su http://www.dyndns.org/. Sono supportati differenti servizi DDNS (fare riferimento all'appendice H).
- **Virtual Server:** L'utente può specificare alcuni servizi da rendere disponibili per utenti esterni. Il Wireless Broadband Router può riconoscere le richieste entranti di questi servizi e rigirarle all'opportuno PC della Lan. E' possibile, per esempio, assegnare una data funzione ad un PC della Lan (come server Web) e renderlo disponibile in Internet (tramite l'unico IP statico disponibile). Dall'esterno è così possibile accedere al server Web che resta comunque protetto dal NAT. Grazie all'uso della tecnologia DDNS non è necessario che il Router abbia un abbonamento con IP fisso.
- **Dynamic Host Control Protocol (DHCP) client and server:** Lato WAN, il dispositivo può, grazie al DHCP client, prendere un indirizzo IP dall'ISP automaticamente. Nella LAN, il DHCP server può gestire sino a 253 client IP, distribuendo a ciascun PC un indirizzo IP, la subnet mask ed i DNS. Questa funzionalità consente una facile gestione della Lan.
- **Mac Filtering:** Tramite questa funzionalità è possibile filtrare ulteriormente il traffico limitando l'accesso in base all'indirizzo MAC degli apparati di rete. Sarà possibile bloccare l'accesso ad una lista di MAC Address.
- **UPnP:** Grazie alla funzionalità UPnP è possibile configurare facilmente tutte quelle applicazioni che hanno problemi nell'attraversamento del NAT. L'utilizzo del NAT Trasversale renderà le applicazioni in grado di configurarsi automaticamente senza l'intervento dell'utente. Chiunque dunque sarà in grado, senza conoscere complicati concetti, di godere pienamente dei vantaggi del NAT e contemporaneamente utilizzare le più comuni applicazioni Internet senza il minimo problema.
- **Configurabile (GUI) via Web:** La gestione e la configurazione sono possibili via interfaccia grafica (browser).
- **Firmware Upgrade:** E' possibile effettuare l'upgrade del firmware tramite interfaccai WEB.
- **One Touch Configuration**:** Il pieno supporto delle specifiche Wi-Fi Protected Setup^{TM} permettono la configurazione e la messa in sicurezza della propria rete senza fili mediante la sola pressione di un pulsante. Questo rende il prodotto la soluzione ideale anche per l'home-user meno esperto.

* = Le prestazioni possono subire variazioni in base ai client e alla configurazione utilizzata.

** = Questa funzionalità è utilizzabile solo con i client che supportano le specifiche Wi-Fi Protected Setup™.

1.4 Requisiti di Sistema per la configurazione

Prima di iniziare l'installazione del dispositivo controllare i seguenti requisiti:

- Un Computer con un qualsiasi Sistema Operativo e lo stack TCP/IP correttamente installato
- Internet Explorer V6.0 o successivi (Netscape V6.0 o successivi)
- CDRom

1.5 Schema di installazione del prodotto

Di seguito è riportato una procedura consigliata, al fine di facilitare l'installazione fisica del dispositivo:

1. Il WebShare RB300 può essere collegato, tramite la porta RJ-45 (LAN) alla rete o al PC, e tramite la porta WAN al Router/Modem ADSL (es: A01-AE1) o al dispositivo responsabile della connettività (nel caso di connettività su cavo).
2. Collegare l'alimentatore AC-DC (2.5A/5V) alla rete elettrica ed al prodotto tramite l'apposito jack, utilizzando l'apposito attacco DC-IN situato sul pannello posteriore del prodotto.

E' possibile vedere in figura un esempio di cablaggio di una rete con diversi PC.

1.6 Considerazioni sull'Installazione

In condizioni ideali, la copertura offerta dal dispositivo può arrivare anche a coprire un raggio molto vasto (si consideri che il prodotto è in grado di fornire fino a 10 volte la copertura di un AccessPoint IEEE 802.11g).
E' però opportuno considerare che pareti divisorie attenuano fortemente il segnale e che oggetti di natura o struttura metallica riflettono le onde elettromagnetiche e possono generare fastidiosi cammini multipli.
Non va trascurato inoltre il fenomeno dell'interferenza con altri apparati operanti sulle frequenze vicine (soprattutto nel caso in cui si utilizzi la modalità a doppio canale).
E' consigliato il rispetto dei seguenti punti per massimizzare la copertura offerta dal dispositivo:

- Ogni muro attenua il segnale; è consigliato posizionare il dispositivo in un luogo appropriato al fine di minimizzare il numero di muri attraversati dal segnale.
- Porte o ampie superfici metalliche non sono attraversate dalla propagazione elettromagnetica.
- Allontanare il Webshare RB300 da ogni altro dispositivo che produca emissioni RF.
- Nel caso di trasmissioni radio con utilizzo della tecnologia MIMO, è necessario valutare il corretto posizionamento delle antenne e l'indentificazione del punto di accesso all'interno dell'ambiente di distribuzione
  Nel posizionamento dei vari client considerare una linea che idealmente unisce il Wireless Broadband Router col client in questione. Se tale linea intersecherà dei muri (caso assai frequente), cercare di minimizzare la superficie attraversata (per evitare di avere un'attenuazione importante).

Si ricorda inoltre che, al fine di rispettare i limiti normativi del paese di utilizzo, non è consigliato sostituire le antenne fornite a corredo con antenne di guadagno superiore.

CAPITOLO 2: Utilizzo del WebShare RB300

2.1 Precauzioni nell'uso del Wireless Broadband Router

- Non utilizzare il Wireless Broadband Router in un luogo in cui ci siano condizioni di alte temperatura ed umidità; il Wireless Broadband Router potrebbe funzionare in maniera impropria e danneggiarsi.
- Non utilizzare la stessa presa di corrente per connettere altri apparecchi al di fuori del Wireless Broadband Router.
- Non aprire mai il case del Wireless Broadband Router né cercare di ripararlo da soli; queste operazioni invalideranno la garanzia del prodotto.
- Se il Wireless Broadband Router dovesse presentare segnali di surriscaldamento (superficie plastica eccessivamente calda), è consigliato lo spegnimento immediato e successivamente rivolgersi a personale qualificato.
- Non appoggiare il dispositivo su superfici plastiche o in legno che potrebbero non favorire lo smaltimento termico e/o la corretta aerazione del prodotto.
- Installare il Wireless Broadband Router su una superficie piana e stabile oppure fissarlo a muro tramite le apposite scanalature sul pannello inferiore.
- Usare esclusivamente l'alimentatore fornito a corredo; l'uso di altri alimentatori farà automaticamente decadere la garanzia.
- Non effettuare aggiornamenti di firmware utilizzando apparati/client wireless ma solo wired. Interferenze o cadute di connessione durante l'aggiornamento potrebbero danneggiare il dispositivo ed invalidare la garanzia.
- Non sostituire le antenne fornite in dotazione con antenne con guadagno superiore; questo permetterà al dispositivo di lavorare in piena conformità con la normativa vigente in merito alle trasmissioni in radiofrequenza.

2.2 I LED frontali

Sul pannello frontale del Wireless Broadband Router sono presenti tutta una serie di Led che indicano lo stato di alcune funzionalità del prodotto.
L'immagine e la tabella seguenti descrivono i LED posti sul pannello frontale del Wireless Broadband Router.

LED	INFORMAZIONE
POWER	Acceso fisso quando connesso alla rete elettrica.
STATUS	• Lampeggiante quando il dispositivo funziona correttamente. • Acceso verde fisso o spento quando il dispositivo ha problemi.
WAN	• Acceso quando connesso ad un dispositivo Ethernet • Lampeggiante quando vi è trasmissione/ricezione.
WLAN	• Acceso lampeggiante quando il modulo wireless è correttamente caricato e quando vi è trasmissione/ricezione. • Spento se il modulo wireless è disattivato.
LAN (1-4)	• Acceso quando connesso ad un dispositivo Ethernet • Lampeggiante quando vi è trasmissione/ricezione.

2.3 Le porte posteriori

PORTE	UTILIZZO
POWER	Connettere l'alimentatore a questo jack.
WAN	Connettere con un cavo UTP.
LAN	Connettere con un cavo UTP.
CONNETTORI SMA	Collegare l'antenna fornita in dotazione.
RESET	• A dispositivo acceso, premere per circa 12 sec. per effettuare il reset del prodotto; rilasciare e questo punto il bottone. Tutti i LED si accenderanno e poi il sistema effettuerà un reboot caricando i parametri di default. • A dispositivo acceso, premere per circa 2 sec per effettuare il riavvio del dispositivo. • A dispositivo spento, premere il pulsante e collegare l'alimentazione; mantenere premuto per circa 12 sec per attivare la procedura di recovery.

2.4 Cablaggio

Anzitutto collegare alle porte RJ45 i PC della Lan oppure ulteriori Switch. Infine collegare l'alimentatore al Router ed alla presa elettrica. Una volta effettuati tutti i collegamenti, il prodotto effettuerà una diagnostica la cui durata è di circa una decina di secondi. Terminata questa fase, il Led POWER sarà acceso verde fisso ed il Led STATUS comincerà a lampeggiare indicando il corretto funzionamento del prodotto. I Led LAN/WLAN/WAN saranno accesi (a seconda dei collegamenti fatti) o lampeggianti .
In figura è possibile osservare una tipica installazione domestica, sulla cui porta WAN dell'apparato è stato collegato un dispostivo A02-RA141/A02-RA111 responsabile della connettività ADSL2+.

CAPITOLO 3: Configurazione

Il Wireless Broadband Router può essere configurato via browser Web che dovrebbe essere incluso nel Sistema Operativo o comunque facilmente reperibile in Internet. Il prodotto offre una semplice interfaccia di configurazione.

3.1 Prima di iniziare

Questa sezione descrive la configurazione richiesta dai singoli PC connessi alla LAN cui è connesso il Wireless Boradband Router . Tutti i PC devono avere una scheda di rete Ethernet installata correttamente, essere connessi al Wireless Broadband Router direttamente in wired/wireless o tramite un Hub/Switch ed avere il protocollo TCP/IP installato e correttamente configurato in modo da ottenere un indirizzo IP tramite il DHCP Server residente sul prodotto. Nel caso in cui il PC abbia già un indirizzo IP, questo deve stare nella stessa subnet del Wireless Broadband Router (il cui indirizzo IP di default è 192.168.1.1 e subnet mask 255.255.255.0). Certamente la strada più semplice per configurare i PC è quella settarli come client DHCP cui l'IP (ed altri parametri) è assegnato dal Wireless Broadband Router .
Anzitutto è necessario preparare i PC inserendovi (qualora non ci fosse già) la scheda di rete wired. E' necessario poi installare il protocollo TCP/IP. Qualora il TCP/IP non fosse correttamente configurato, seguire gli steps successivi:

NOTE: Qualsiasi workstation col TCP/IP può essere usata per comunicare con o tramite il Wireless Broadband Router. Per configurare altri tipi di workstations fare riferimento al manuale del produttore.

3.1.1 Configurazione del PC in Windows 95/98/ME

1. Andare in **Start/Settings/Control Panel**.
2. Cliccare 2 volte su **Network** e scegliere **Configuration**.
3. Selezionare **TCP/IP -> NE2000 Compatible**, o qualsiasi Network Interface Card (NIC) del PC.
4. Cliccare su **Properties**.
5. Selezionare l'opzione **Obtain an IP address automatically** (dopo aver scelto IP Address).
6. Andare su **DNS Configuration**
7. Selezionare l'opzione **Disable DNS**.

Provvedere al riavvio della macchina al fine di apportare le modifiche effettuate.

3.1.2 Configurazione del PC in Windows NT4.0

1. Andare su **Start/Settings/ Control Panel**.
2. Cliccare per due volte su **Network** e poi cliccare su **Protocols**.
3. Selezionare **TCP/IP Protocol** e poi cliccare su **Properties**.
4. Selezionare l'opzione **Obtain an IP address from a DHCP server** e premere **OK**.

3.1.3 Configurazione del PC in Windows 2000

1. Andare su Start**/Settings/Control Panel**.
2. Cliccare due volte su **Network and Dial-up Connections.**
3. Cliccare due volte su **Local Area Connection**.
4. In Local Area Connection Status cliccare **Properties**.
5. Selezionare **Internet Protocol (TCP/IP)** e cliccare su **Properties**
6. Selezionare l'opzione **Obtain an IP address automatically**
7. Selezionare l'opzione **Obtain DNS server address automatically**
8. Premere su **OK** per terminare la configurazione

3.1.4 Configurazione del PC in Windows XP

1. Andare su **Start/Control Panel**.
2. Cliccare due volte su **Network Connections (in Classic View)**.
3. Cliccare due volte su **Local Area Connection**.
4. In Local Area Connection Status cliccare **Properties**.
5. Selezionare **Internet Protocol (TCP/IP)** e cliccare su **Properties**.
6. Selezionare l'opzione **Obtain an IP address automatically**
7. Selezionare l'opzione **Obtain DNS server address automatically**
8. Premere su **OK** per terminare la configurazione

3.1.5 Configurazione in Windows VISTA

1. Andare su **Start/Pannello di Controllo**
2. Dopo aver cliccato sulla voce Visualizzazione classica, cliccare due volte sull'icona **Centro Connessione di rete e Condivisione**.
3. Cliccare su **Gestisci connessione di rete**.
4. Cliccare 2 volte sull'icona **Local Area Connection** e cliccare su Proprietà nel caso in cui sia richiesto, cliccare su Si per fornire l'autorizzazione dell'utente).
5. Selezionare **Protocollo Internet Versione 4 Protocol (TCP/IPv4)** e cliccare su **Proprietà**.
6. Selezionare l'opzione **Ottieni automaticamente un indirizzo IP**
7. Selezionare l'opzione **Ottieni indirizzi server DNS automaticamente**.
8. Premere su **OK** per terminare la configurazione.

3.1.6 Configurazione in ambiente MAC

1. Cliccare sull'icona Mela nell'angolo in alto a sinistra dello schermo e selezionare **Control Panel/TCP/IP**.
2. Scegliere **Ethernet in Connect Via**.
3. Scegliere **Using DHCP Server** in **Configure**.
4. Lasciare vuoto il campo **DHCP Client ID**.

3.1.7 Verifica della Configurazione

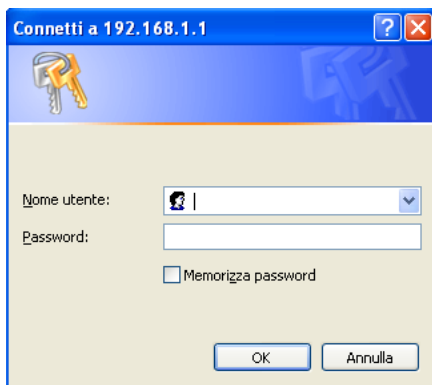
Per verificare il successo della configurazione (dopo aver riavviato il PC, operazione necessaria su Win98, 98Se,ME e invece sufficiente ottenere il rilascio dell'IP su XP, 2000), utilizzare il comando ping. Da una finestra Dos digitare:
ping 192.168.1.1
Se appare il seguente messaggio:

Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 times<10ms TTL=64
Reply from 192.168.1.1: bytes=32 times<10ms TTL=64
Reply from 192.168.1.1: bytes=32 times<10ms TTL=64

E' possibile procedere andando al punto seguente. Se invece appare il seguente messaggio:

Pinging 192.168.1.1 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.

Controllare che il led LAN/WLAN sia acceso (cambiare il cavo qualora non fosse così). Controllare l'indirizzo del PC digitando **winipcfg** per (Win95,98,ME) o **ipconfig** (per Win2000,XP) ed eventualmente reinstallare lo stack TCP/IP.

3.2 Settaggi di Default

Prima di iniziare la configurazione del prodotto, è necessario i seguenti paramentri di base:

- Nome Utente: **admin**
- Password: **admin**
- Indirizzo IP: **192.168.1.1**
- Subnet Mask: **255.255.255.0**
- Indirizzo IP WAN: **client DHCP**
- DHCP Server: **abilitato (192.168.1.100-192.168.1.199)**
- SSID: **N Router**

- Channel: **6**,
- Sicurezza: **disabilitato**

3.2.1 Password

Quando si configura Il Wireless Broadband Router con il browser, introdurre username e password e premere su OK per entrare per la prima volta.

E' consigliato cambiare la password, al fine di aumentare la sicurezza.

Qualora si perdesse la password premere per 10 (o più) secondi il bottone reset (utilizzando un cacciavite a punta e premendo delicatamente) per far tornare il Wireless Broadband Router alle impostazioni di default.

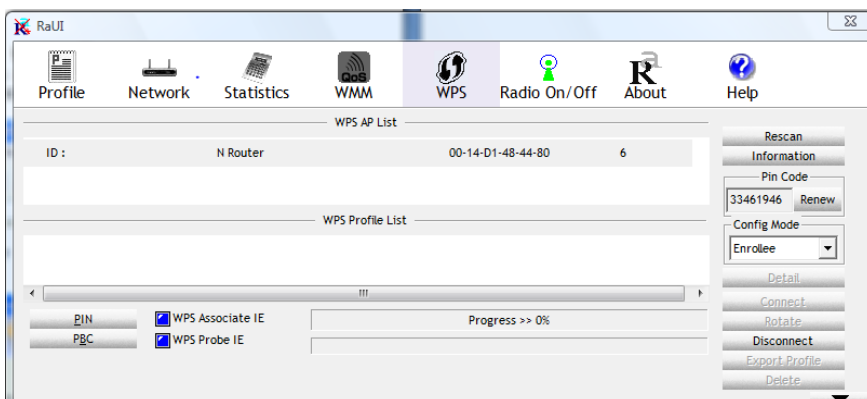
3.2.2 Porte LAN e WLAN

Questa tabella riassume i settaggi di default delle interfacce LAN e WLAN:

Porta LAN		Porta WLAN
IP address	192.168.1.1	Canale=**6** SSID=**N Router** Sicurezza=**Disabilitata**
Subnet Mask	255.255.255.0	

3.3 OneTouch Configuration

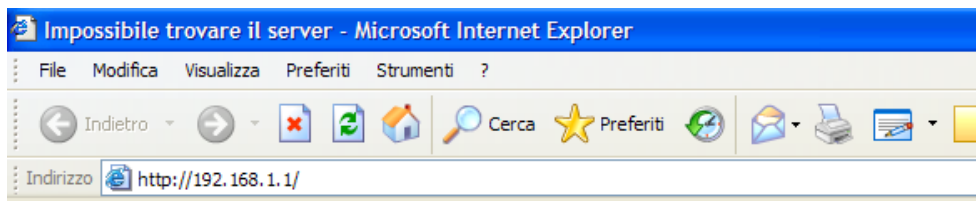
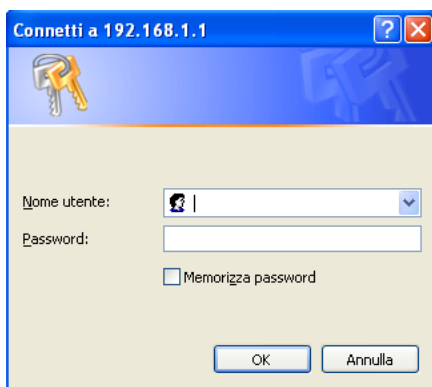
Grazie alla tecnologia OneTouch Configuration** (pienamente supportata da tutta la gamma NetFly 300 di Atlantis Land), è possibile configurare la propria rete wireless tramite la pressione di un pulsante*.
Per effettuare la configurazione tramite OneTouch, seguire la procedura indicata di seguito:

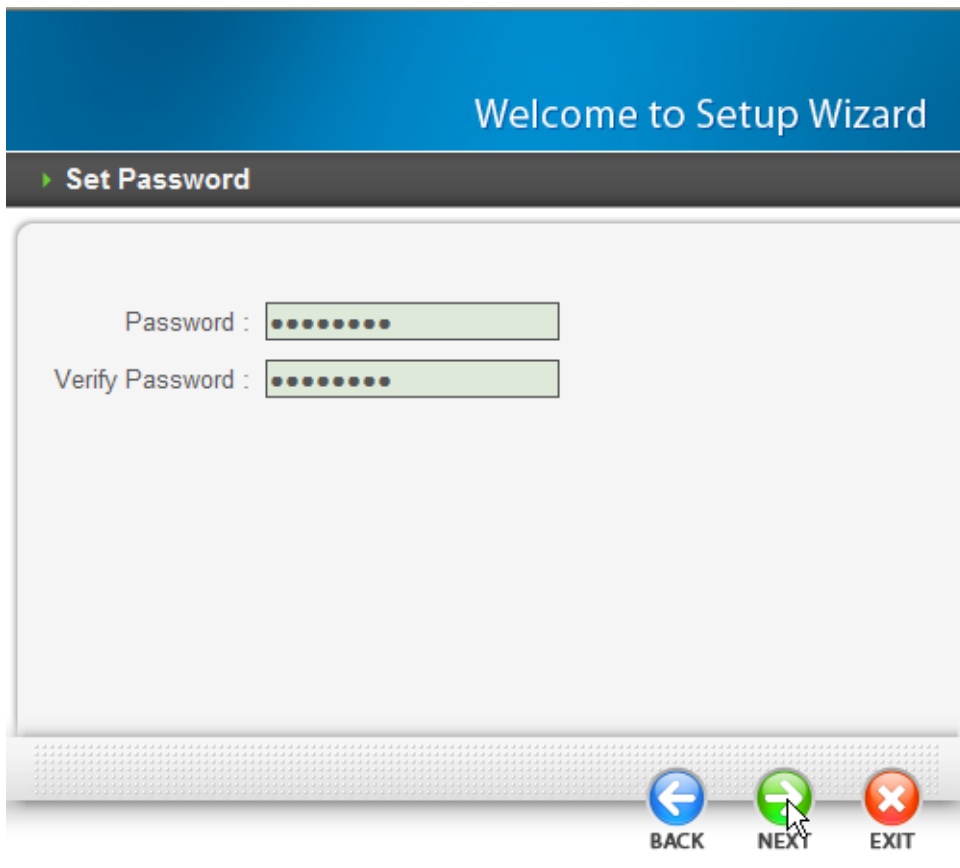
1. Premere il pulsante WPS posto sul lato destro del prodotto (vista frontale); lo stesso indicherà l'attivazione della modalità di sincronizzazione tramite un lampeggio regolare del pulsante.
2. Accedere all'utility di configurazione del client (A02-UP-W300N o A02-PCI-W300N) e verificare la presenza della rete senza fili con SSID "N Router" sotto la voce WPS -> WPS AP List.

3. Premere il pulsante PCB ed attendere la sincronizzazione del client con il WebShare RB300. La barra di progresso indicherà, in maniera percentuale, lo stato di esecuzione della sincronizzazione.

Al termine della sincronizzazione, sotto la sezione WPS Profile List sarà possibile verificare il nuovo profilo di connessione generato dal prodotto; selezionando il profilo e premendo su **Detail** sarà possibile visualizzare i dettagli relativi allo stesso.
Premendo su **Export Profile** sarà possibile esportare il profilo WPS creato tra i profili di connessione, al fine di permettere la riconnessione automatica del client al dispositivo in caso di caduta della stessa.

** = Questa funzionalità è utilizzabile solo con i client che supportano le specifiche Wi-Fi Protected Setup™.

3.4 Configurazione tramite Browser

Accedere tramite Internet Explorer al seguente indirizzo IP (dove si inserisce l'URL) che di default è: "**192.168.1.1**", e premere il tasto invio.

Introdurre il nome utente e la password (**admin**, **admin**) e premere **OK** per continuare.

Apparirà a questo punto l'interfaccia di configurazione dell'apparato.
Chiudendo la Wizard è possibile accedere al Menù Principale dove è possibile configurare dettagliatamente il dispositivo (saltare la sezione immediatamente seguente). Nel caso il Wizard non fosse presente è sufficiente cliccare sull'apposita voce per avviarlo.

3.4.1 Setup Wizard

Grazie a questo Wizard è possibile configurare il dispositivo in brevissimo tempo. Apparirà l'immagine di sotto (qualora non fosse così, cliccare sul bottone Wizard).

Welcome to Setup Wizard

Setup Wizard

Step 1. Set your New Password
Step 2. Choose your Time zone
Step 3. Set LAN Connection and DHCP Server
Step 4. Set Internet Connection
Step 5. Set wireless connection
Step 6. Restart

Display Wizard next time? Yes No

NEXT EXIT

Cliccare su **Next** per proseguire.

Step 1: Set Password

Inserire la password di accesso per l'utente amministratore (admin); durante la prima configurazione è consigliato cambiare la password di accesso al fine di impedire tentativi di accesso non desiderati.

Cliccare su **Next** per proseguire.

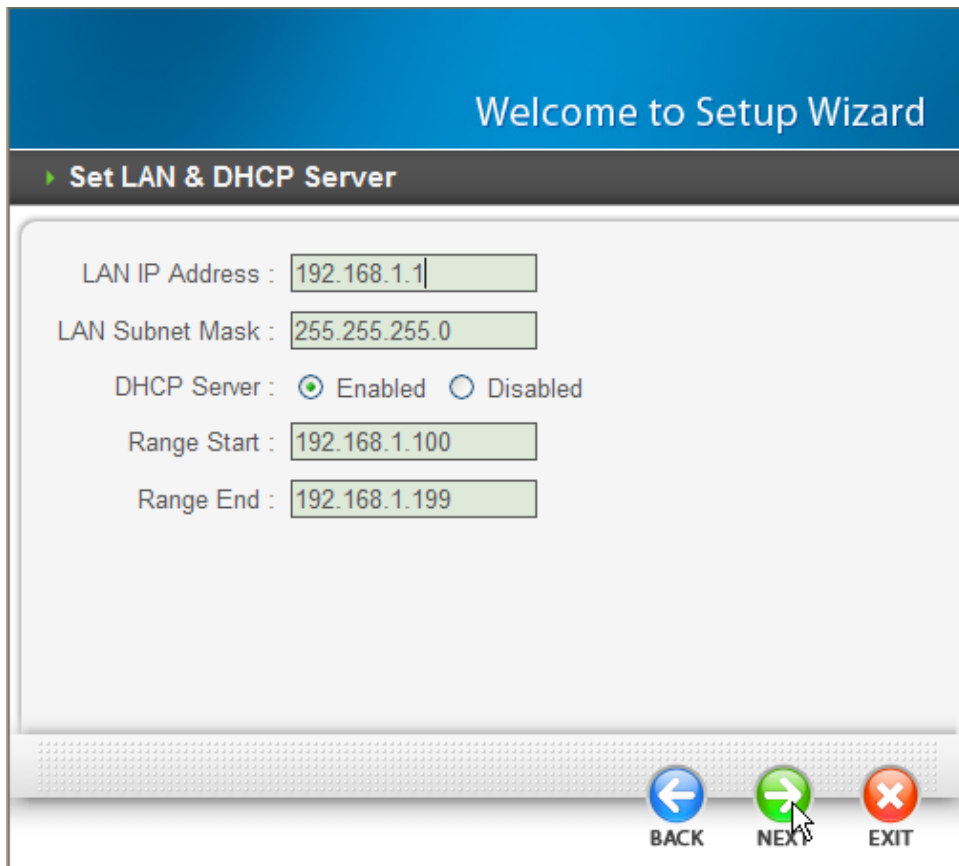
Step2: Choose Time Zone

Selezionare adesso dal menù a tendina la fascia oraria di appartenenza (la corretta selezione di questo parametro permetterà la corretta temporizzazione e la corretta registrazione degli eventi di log).

Welcome to Setup Wizard

Choose Time Zone

(GMT+01:00) Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna

BACK NEXT EXIT

Cliccare su **Next** per proseguire.

Step 3: Set LAN & DHCP Server
E' possibile cambiare l'indirizzo IP del dispositivo e la maschera di rete.
Spuntare **Enabled** per abilitare il DHCP server del dispositivo, in modo che questo assegni in maniera automatica gli indirizzi IP ai vari client Wireless o Wired. Tramite i campi **Range Start** e **Range End** è possibile assegnare il range di IP che saranno assegnati dal servizio DHCP Server.

Welcome to Setup Wizard

Set LAN & DHCP Server

LAN IP Address : 192.168.1.1
LAN Subnet Mask : 255.255.255.0
DHCP Server : Enabled Disabled
Range Start : 192.168.1.100
Range End : 192.168.1.199

BACK NEXT EXIT

Cliccare su **Next** per continuare.

Step 4: Select Internet Connection Type

In questa sezione del processo di configurazione, sarà possibile selezionare la modalità di connessione ad Internet tra le 6 scelte disponibili. Se il dispositivo è utilizzato come Access Point (la porta WAN non viene collegata a nessun dispositivo in grado di fornire connettività), si consiglia di saltare allo step (5) successivo.

Welcome to Setup Wizard

Select Internet Connection Type

- (•) Obtain IP automatically (DHCP client)
- ( ) Fixed IP
- ( ) PPPoE
- ( ) PPTP
- ( ) L2TP
- ( ) BigPond

BACK NEXT EXIT

Cliccare su **Next** per continuare.

Set Dynamic IP Address:
Scegliendo **Obtain IP automatically (DHCP client)**, l'interfaccia WAN otterrà un indirizzo IP da un server DHCP presente sulla rete cui viene collegata.

A questo punto, è possibile clonare sul Wireless Broadband Router un indirizzo MAC particolare.
Nel caso non ci fosse questa necessità proseguire cliccando **Next**.

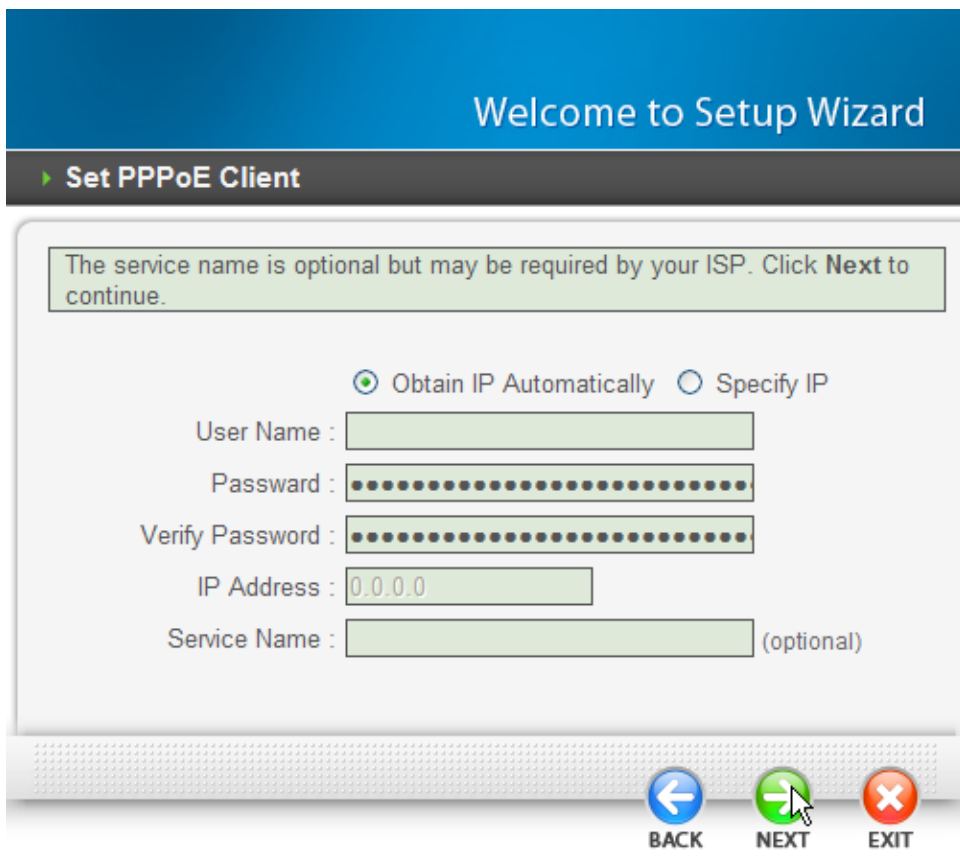
Set Fixed IP Address:
Introdurre l'indirizzo IP, maschera di rete e Gateway da assegnare all'interfaccia WAN.

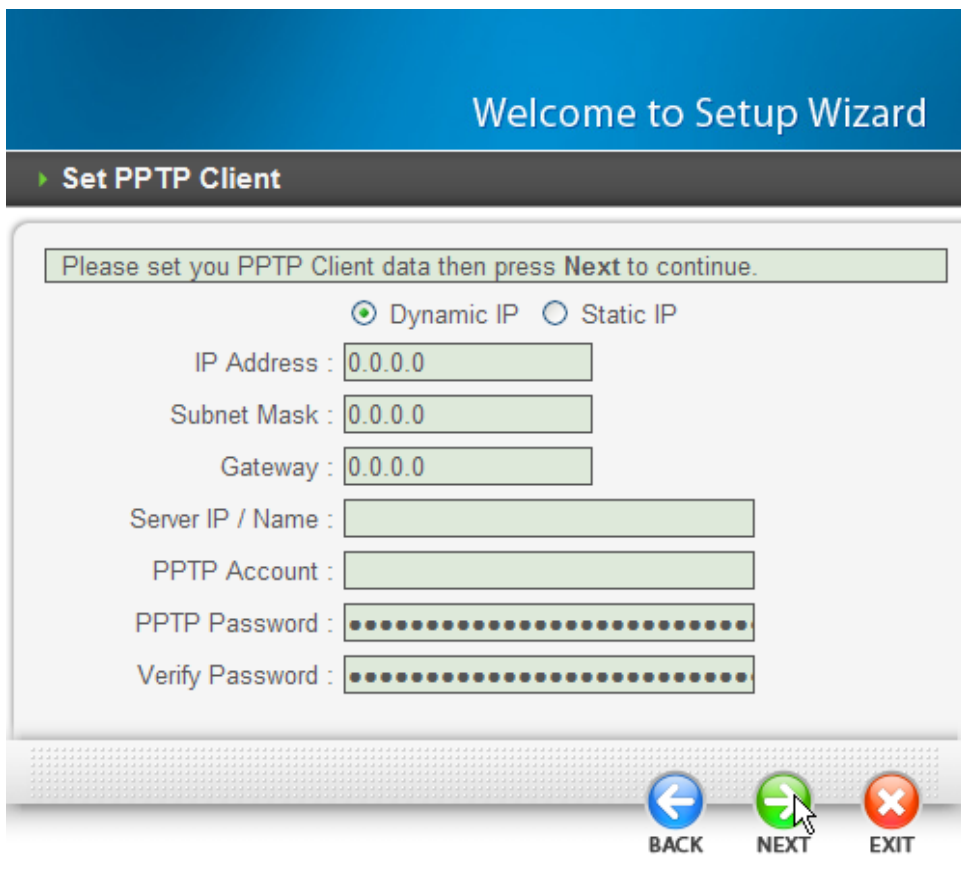
Welcome to Setup Wizard

Set Fixed IP Address

Enter in the static IP information provided to you by your ISP. Click **Next** to continue.

WAN IP Address : 0.0.0.0
WAN Subnet Mask : 0.0.0.0
WAN Gateway Address : 0.0.0.0
DNS Server Address 1 : 0.0.0.0
DNS Server Address 2 : 0.0.0.0

BACK NEXT EXIT

Si ricorda che utilizzando questa modalità, è necessario introdurre gli indirizzi IP dei server DNS da utilizzare.
Cliccare su **Next** per continuare.

Set PPPoE Client:
Introdurre l'Username e Password (ed il Service Name se espressamente richiesto dal fornitore del servizio) necessari per l'autenticazione del profilo PPPoE (sarà necessario reintrodurre la password per la verifica).
Nel caso fosse necessario un indirizzo IP statico, spuntare la voce **Specify IP** ed immettere nel campo IP Address il valore dello stesso.

Cliccare su **Next** per continuare.

Set PPTP/L2TP Client:
Introdurre Username e Password da utilizzare per l'autenticazione del profilo PPTP/L2TP ed il nome/indirizzo IP del server PPTP responsabile della connessione.
Spuntare la voce **Static IP** nel caso in sia richiesto un indirizzamento IP statico da assegnare al client PPTP/L2TP.

Welcome to Setup Wizard

Set PPTP Client

Please set you PPTP Client data then press **Next** to continue.

Dynamic IP   Static IP

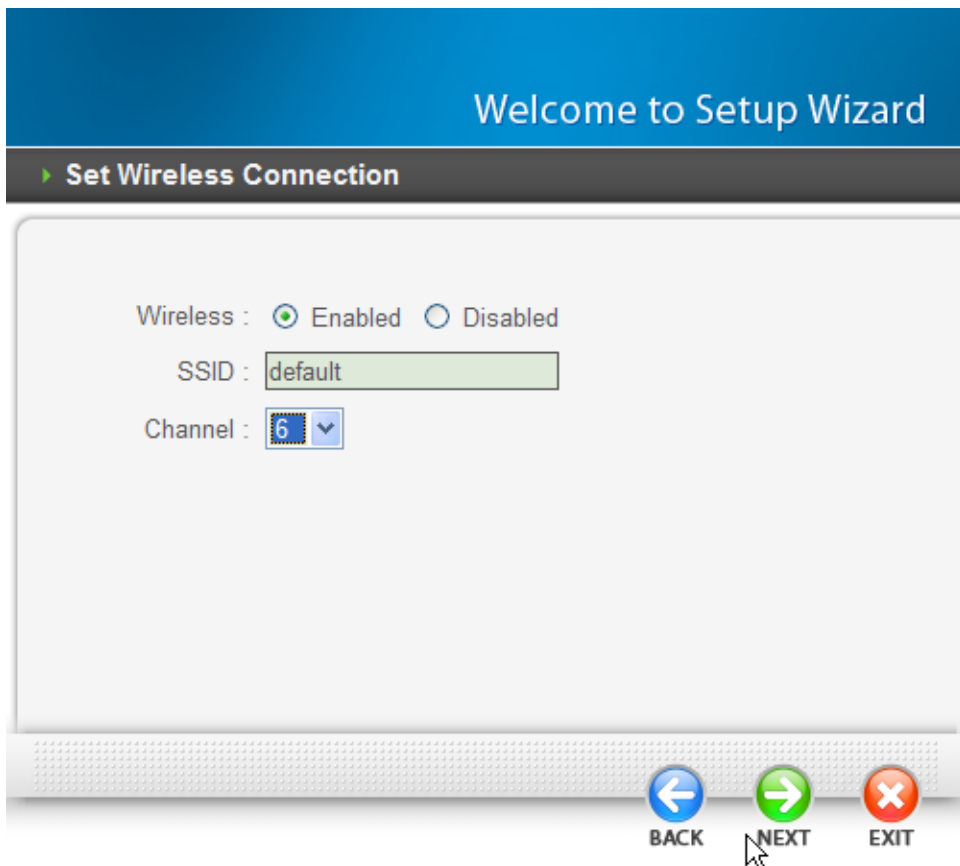
IP Address : 0.0.0.0

Subnet Mask : 0.0.0.0

Gateway : 0.0.0.0

Server IP / Name :

PPTP Account :

PPTP Password :

Verify Password :

BACK   NEXT   EXIT

Cliccare su **Next** per continuare.

Step 5: Set Wireless LAN connection

Cliccare **Enabled** per abilitare l'interfaccia radio; introdurre l'SSID (servirà come identificativo della rete e dovrà essere identico per tutti i dispositivi) e scegliere il canale di trasmissione per il dispositivo.

Welcome to Setup Wizard

Set Wireless Connection

Wireless : Enabled Disabled

SSID : default

Channel : 6

BACK NEXT EXIT

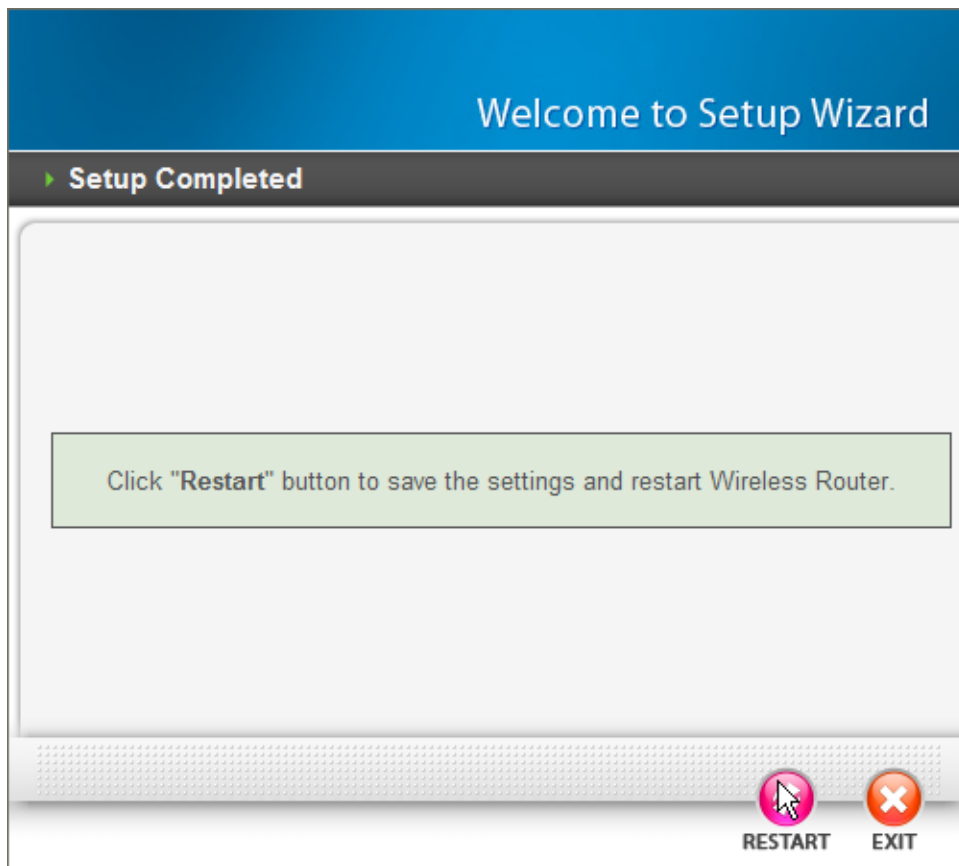
Cliccare su **Next** per continuare.

Step 6: Restart
A questo punto la configurazione è terminata; riavviare il Wireless Broadband Router premendo su **Restart**. Cliccando invece su **Exit** tutti i settaggi impostati non verranno salvati.

Welcome to Setup Wizard

Setup Completed

Click "**Restart**" button to save the settings and restart Wireless Router.

RESTART EXIT

A questo punto, effettuare una prova di navigazione per verificare l'esito positivo della configurazione appena effettuata.

3.4.2 Navigare nell'interfaccia Web di Configurazione

Questa sezione descrive come navigare all'interno dell'interfaccia di configurazione.

Sono disponibili 6 differenti menu:

- **WAN**
- **Wireless**
- **LAN**
- **Access Control**
- **System**
- **Wizard**

3.5 WAN

3.5.1 Connection Type

In questa sezione è possibile configurare l'interfaccia WAN dell'apparato (nel caso di utilizzo del prodotto in modalità Access Point, non sarà necessario configurare questi parametri).

Connection Type

Connection Type : DHCP Client or Fixed IP

WAN IP Address : Obtain IP Automatically Specify IP

IP Address : 192.168.3.100

Subnet Mask : 255.255.255.0

Gateway : 0.0.0.0

DNS 1 : 0.0.0.0

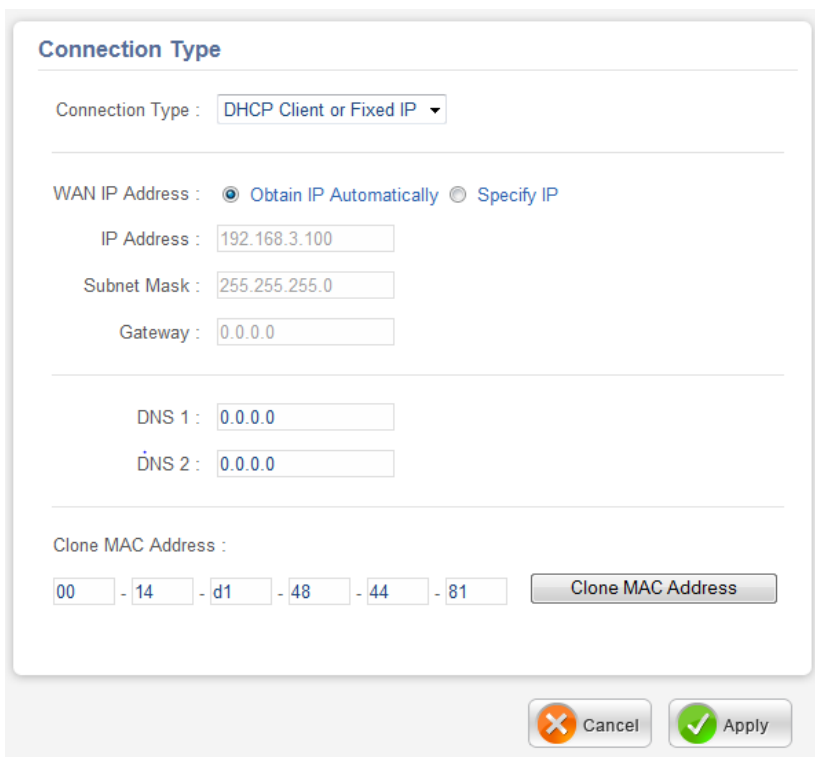
DNS 2 : 0.0.0.0

Clone MAC Address :

00 - 14 - d1 - 48 - 44 - 81 Clone MAC Address

Cancel Apply

Connection Type: E' possibile scegliere tra le seguenti opzioni **DHCP client or Fixed IP**, **PPPoE**, **PPTP**, **L2TP** e **BigPond Cable** presenti nel menù a tendina.

Di seguito sono riportate le configurazioni necessarie per ognuna delle opzioni.

DHCP client or Fixed IP

Selezionando questa modalità, sarà possibile configurare il prodotto in maniera tale da ottenere automaticamente un indirizzamento IP oppure specificare l'indirizzo da assegnare all'interfaccia WAN.

Selezionando la voce **Specify IP**, sarà necessario immettere l'indirizzo IP, maschera di rete, gateway e gli indirizzi dei server DNS.

Selezionando la voce **Obtain IP automatically**, il router riceverà, sull'interfaccia WAN, l'indirizzo IP da un opportuno server DHCP.

E' inoltre possibile clonare un particolare indirizzo MAC inserendolo nel campo apposito e premendo il tasto **Clone MAC Address**.

Connection Type

Connection Type : DHCP Client or Fixed IP

WAN IP Address : Obtain IP Automatically Specify IP

IP Address : 192.168.3.100

Subnet Mask : 255.255.255.0

Gateway : 0.0.0.0

DNS 1 : 0.0.0.0

DNS 2 : 0.0.0.0

Clone MAC Address :

00 - 14 - d1 - 48 - 44 - 81 Clone MAC Address

Cancel Apply

Cliccare su **Apply** per salvare le modifiche.

In caso si selezioni la voce **Specify IP**, è necessario inserire il server DNS primario (DNS Server Address 1).

PPPoE

E' necessario collegare l'apparato ad un modem Ethernet (settato come Bridge) ed introdurre tutti i parametri relativi al collegamento ADSL PPPoE. In questo modo l'indirizzo IP assegnato dall'ISP (dinamico o statico) verrà assegnato all'interfaccia WAN del prodotto, permettendo la condivisione della connessione ai client collegati sulle interfaccie LAN e WLAN.

Connection Type

Connection Type : PPPoE

WAN IP Address : Obtain IP Automatically

Specify IP 0.0.0.0

Service Name :

User Name :

Password :

Verify Password :

MAC Address : - - - - - (optional)

Clone MAC Address

DNS : Primary 0.0.0.0

Secondary 0.0.0.0 (optional)

Auto-reconnect : Always On Manual Connect-on Demand

Idle Time Out : 5 Minutes

MTU : 1492

Cancel Apply

Wan IP Address: Spuntare la voce **Obtain IP automatically** nel caso in cui l'indirizzo IP venga assegnato dinamicamente dall'ISP. Scegliere invece la voce **Specify IP** per inserire manualmente l'indirizzo IP statico.
Service Name: Immettere il valore del campo solo se specificatamente richiesto dall'ISP.
User Name: Inserire il nome utente fornito dall'ISP.
Password: Inserire la password fornita dall'ISP.
Verify Password: Reinserire la password immessa nel campo **Password**.
DNS: Inserire gli indirizzi dei server DNS (vengono richiesti un DNS primario e uno opzionale secondario).
Auto-reconnect: Selezionare la modalità di riconnessione alla rete Internet in caso di caduta temporanea della stessa. E' possibile scegliere tra **Always On, Manual** o **Connect-on Demand.**
Idle Time Out: Immettere un valore (espresso in minuti), al termine del quale, nel caso in cui non venga rilevato alcun passaggio di pacchetti, il Router interromperà la connessione PPPoE (Questa opzione non è verrà utilizzata nella modalità **Always On**).
MTU: Inserire il valore della Maximum Transfert Unit (è consigliabile non modificare il valore proposto).

Cliccare su **Apply** per salvare le modifiche.

Per ulteriori dettagli consultare l'Appendice D. Richiedere tutti i parametri necessari al proprio ISP (Username, password).

Si ricorda che tale dispositivo non è adatto a gestire abbonamenti non FLAT (a consumo). Atlantis Land non potrà essere ritenuta responsabile per qualsiai problematica derivante dall'utilizzo di abbonamenti a consumo (non FLAT) o da una errata configurazione dell'apparato.

In caso di dubbio contattare, prima di effettuare la configurazione del dispositivo, l'assistenza tecnica.

PPTP/L2TP

E' necessariamente collegare l'apparato ad un opportuno modem/Router Ethernet. Per dettagli consultare il manuale dell'apparato e richiedere tutti i dettagli al proprio ISP (Username, password).

Connection Type

Connection Type : PPTP

WAN IP Address : Obtain IP Automatically Specify IP
IP Address : 192.168.3.100
Subnet Mask : 255.255.255.0
Gateway : 0.0.0.0
DNS : 0.0.0.0

Server IP/Name :
PPTP Account :
PPTP Password :
Verify Password :

Auto-reconnect : Always On Manual Connect-on Demand
Idle Time Out : 5 Minutes
MTU : 1400

Cancel Apply

Wan IP Address: Spuntare la voce **Obtain IP automatically** nel caso in cui l'indirizzo IP venga assegnato dinamicamente dall'ISP. Scegliere invece la voce **Specify IP** per inserire manualmente l'indirizzo IP statico.
Server IP / Name: Immettere il valore del campo solo se specificatamente richiesto dall'ISP.
PPTP Account: Inserire il nome utente fornito dall'ISP, necessario per l'autenticazione del profilo PPTP/L2TP.
PPTP Password: Inserire la password fornita dall'ISP.
Verify Password: Reinserire la password immessa nel campo **Password**.
DNS: Inserire gli indirizzi dei server DNS (vengono richiesti un DNS primario e uno opzionale secondario).
Auto-reconnect: Selezionare la modalità di riconnessione alla rete Internet in caso di caduta temporanea della stessa. E' possibile scegliere tra **Always On, Manual** o **Connect-on Demand.**
Idle Time Out: Immettere un valore (espresso in minuti), al termine del quale, nel caso in cui non venga rilevato alcun passaggio di pacchetti, il Router interromperà la connessione PPPoE (Questa opzione non è verrà utilizzata nella modalità **Always On**).
MTU: Inserire il valore della Maximum Transfert Unit (è consigliabile non modificare il valore proposto).

Cliccare su **Apply** per salvare le modifiche.

Si ricorda che tale dispositivo non è adatto a gestire abbonamenti non FLAT (a consumo). Atlantis Land non potrà essere ritenuta responsabile per qualsiai problematica derivante dall'utilizzo di abbonamenti a consumo (non FLAT) o da una errata configurazione dell'apparato.

In caso di dubbio contattare, prima di effettuare la configurazione del dispositivo, l'assistenza tecnica.

La configurazione per il client BigPond è stata omessa in quanto non presente nel panorama di offerte nazionale.

3.5.2 Dynamic DNS

In questa sezione è possibile configurare un account Dynamic DNS.

Per il corretto utilizzo di questa funzionalità, è necessario registrare preventivamente un dominio DDNS. Fare riferimento all'**APPENDICE H** per un esempio di registrazione.

Dynamic DNS

DDNS : Enabled Disabled

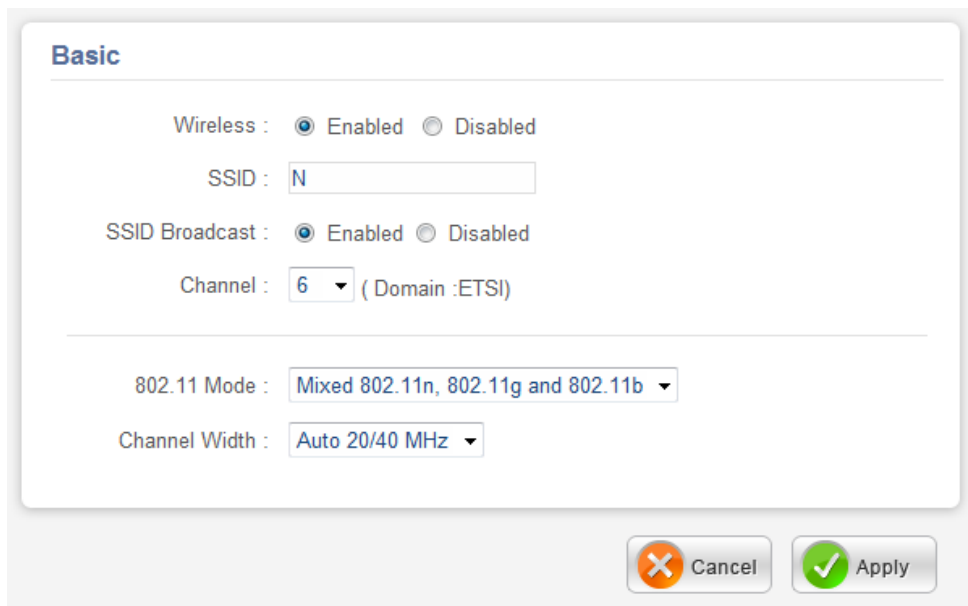
DDNS Server Selection List : DynDns.org

Host Name :

User Name :

Password :

Cancel Apply

DDNS: Cliccare **Enabled** per abilitare il client Dynamic DNS.
DDNS Server Selection List: Selezionare dalla lista il Server DDNS da utilizzare.
Host Name: Inserire l'host Dynamic DNS da utilizzare (è necessario che il dominio sia stato preventivamente registrato sul sito del fornitore di servizio).
User Name: Inserire la UserName necessaria per l'autenticazione dell'account Dynamic DNS.
Password: Inserire la password necessaria per l'autenticazione dell'account Dynamic DNS.

Cliccare su **Apply** per salvare le modifiche.

3.6 Wireless

3.6.1 Basic

In questa sezione è possibile configurare tutti i parametri di base relativi all'interfaccia radio dell'apparato.

Basic

Wireless : Enabled Disabled

SSID : N

SSID Broadcast : Enabled Disabled

Channel : 6 (Domain :ETSI)

802.11 Mode : Mixed 802.11n, 802.11g and 802.11b

Channel Width : Auto 20/40 MHz

Cancel Apply

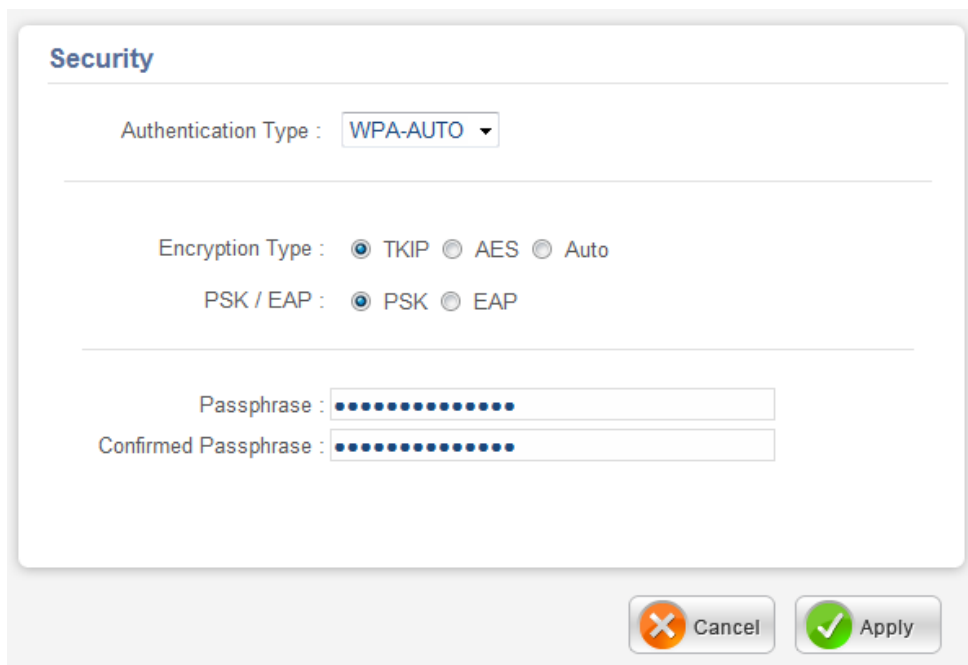
Wireless: Cliccare **Enable** per abilitare l'interfaccia wireless.
SSID: Introdurre il valore di SSID. Questo valore, identificativo della rete wireless, verrà visualizzato dai client durante lo scan delle reti disponibili.
SSID Broadcast: Cliccare su **Enable** per abilitare la modalità di broadcast per l'SSID. Nel caso si desider che l'SSID della rete non venga visualizzato durante uno scanning delle reti disponibili, selezionare **Disable**.
Channel: Selezionare il canale da utilizzare per la trasmissione wireless. Per ulteriori informazioni sulla scelta corretta del canale di trasmissione, si prega di fare riferimento alla parte di troubleshooting presente alla fine di questo documento.
802.11 Mode: Selezionare la modalità di trasmissione del prodotto tra le 3 modalità esclusive (802.11n, 802.11g ed 802.11b) oppure tra le 2 modalità ibride (802.11b/g e 802.11n/g/b). La non corretta selezione di questo parametro può causare problemi di incompatibilità coi i client presenti nella rete.

Channel Width: Selezionare l'ampiezza di canale da utilizzare nella trasmissione radio.

Selezionando la modalità Auto 20/40 MHz, il dispositivo sceglierà in maniera autonoma quale ampiezza di canale utilizzare, in base all'ambiente di lavoro ed all'eventuale presenza di altre reti senza fili.
E' importante ricordare che, nel caso di sovrapposizione e/o interferenza, il dispositivo provvederà a ridurre l'ampiezza di canale a 20 MHz al fine di minimizzare questi effetti.

La velocità massima di trasmissione può essere raggiunta solo nel caso in cui il prodotto trasmetta in ambiente libero da interferenze, utilizzando un canale libero con ampiezza pari a 40 MHz e con client compatibili alle specifiche 802.11n.
Nel caso in cui una delle suddette condizione venisse a mancare, è possibile rilevare decrementi prestazionali in termini di throughput.

Cliccare su **Apply** per salvare le modifiche.

Il range di frequenze radio usate dalle apparecchiature Wireless IEEE 802.11g/b è suddiviso in "canali". Il numero di canali disponibili dipende dall' area geografica di appartenenza. E' possibile selezionare canali differenti in modo da eliminare eventuali interferenze con gli Access Point/ Wireless Broadband Router vicini. L'interferenza si verifica quando due o più canali si sovrappongono degradando le prestazioni, questa sovrapposizione è chiamata "Overlap".
E' consigliabile mantenere una distanza di 5 canali tra due utilizzati (es. AP1 posizionato sul canale 1, AP2 posizionato sul canale 6).

Da questo si evince che soltanto 3 Access Point/Wireless Router possono essere usati in caso di sovrapposizioni spaziali (copertura) e temporali (funzionamento contemporaneo).

3.6.2 Security

Il prodotto supporta i più recenti standard di sicurezza per quanto riguarda le trasmissioni wireless (WEP, WPA e WPA2) .
In questa sezione è possibile configurare le impostazioni di sicurezza legate all'interfaccia wireless dell'apparato.

Security

Authentication Type : WPA-AUTO

Encryption Type : TKIP AES Auto

PSK / EAP : PSK EAP

Passphrase : •••••••••••••••

Confirmed Passphrase : •••••••••••••••

Cancel Apply

Authentication Type: Selezionare la modalità di crittografia da utilizzare. E' possibile scegliere tra: **Disabled**, **WEP**, **WPA**, **WPA2** o **WPA-AUTO**.

Di seguito sono riportate le configurazioni necessarie per ognuna delle opzioni.

WEP

Selezionare questa modalità per utilizzare l'algoritmo WEP (Wired Equivalent Privacy) con chiave statica a 64 o 128 bit. Questo algoritmo risultato particolarmente debole in caso di attacchi a causa della sua struttura, presenta un alto grado di compatibilità con gli standard precedenti (802.11b/g).

Security

Authentication Type : WEP

WEP : Open System Shared Key

WEP Key Format : HEX

WEP Key Length : 64-bit

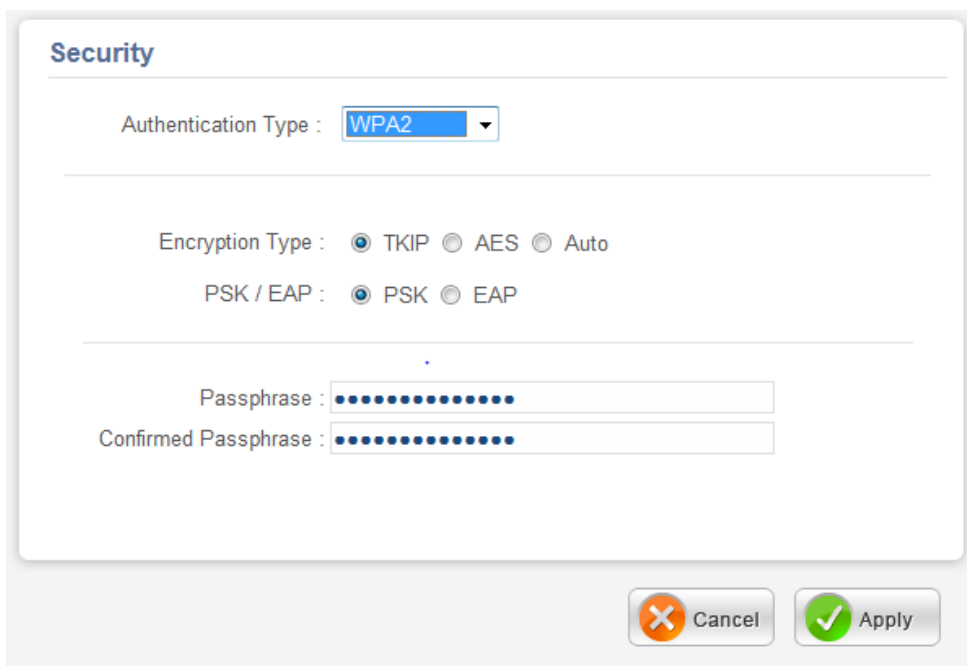
WEP Key 1 : 0000000000

WEP Key 2 : 0000000000

WEP Key 3 : 0000000000

WEP Key 4 : 0000000000

Cancel Apply

WEP: Selezionare la modalità di crittografia tra **Open System** o **Shared Key**.
WEP Key Format: Selezionare il formato delle chiavi da utilizzare.
WEP Key Lenght: Selezionare la lunghezza delle chiavi (64 o 128 bit)
WEP Key 1-4: Introdurre manualmente le 4 chiavi e selezionare quella da utilizzare.

Cliccare su **Apply** per salvare le modifiche.

WPA/WPA2

Selezionare questa modalità per utilizzare l'algoritmo WPA/WPA2 (Wi-Fi Protected Access).

E' possibile scegliere la modalità di autenticazione (chiave precondivisa o RADIUS) e impostare tutti i parametri relativi alla selezione effettuata.

Encryption Type: Selezionare la modalità di cifratura tra **TKIP** o **AES**.
PSK / EAP: Selezionare la modalità di autenticazione tra **PSK** o **EAP** (la modalità EAP richiede un server RADIUS per l'autenticazione).
Passphrase: Inserire la chiave precondivisa da utilizzare.
Confirmed Passphrase: Confermare la chiave immessa nel campo precedente.

Modalità EAP

Questa modalità richiede la presenza di un Radius Server per l'autenticazione dei client. Sarà necessario impostare l'IP del Radius, la porta di comunicazione e la chiave segreta condivisa.

Cliccare su **Apply** per salvare le modifiche.

3.6.3 Advanced

In questa sezione è possibile configurare tutti i dettagli avanzati della connessione wireless.

Advanced

Beacon Interval : 100 (defaule : 100 msec , range : 20 ~ 1000)

RTS Threshold : 2346 (defaule : 2346 , range : 256 ~ 2346)

Fragmentation Threshold : 2346 (defaule : 2346 , range : 1500 ~ 2346)

DTIM Interval : 1 (default : 1, range : 1 ~ 255)

TX Rate : Auto

Antenna Transmit Power: full

Cancel Apply

Beacon Interval: Introdurre nell'apposito spazio un valore numerico. Il valore di default è 100. L'intervallo permesso va da 20ms a 1000ms.
RTS Threshold: Introdurre nell'apposito spazio un valore numerico. Il valore di default è 2436. L'intervallo permesso va da 256 sino a 2436. L'RTS (Request To Send) è un segnale, inviato dalla stazione trasmittente alla stazione ricevente, in cui si richiede il permesso per la trasmissione di dati.
Fragmentation Threshold: Introdurre nell'apposito spazio un valore numerico. Il valore di default è 2346. L'intervallo permesso va da 256 sino a 2346. Cambiando tale valore le performance possono diminuire drasticamente.
DTIM Interval: Introdurre nell'apposito spazio il valore numerico riferito al DTIM (Delivery Traffic Indication Message). Il valore di default è 1. L'intervallo permesso va da 1 sino a 255.

Cliccare su **Apply** per salvare le modifiche.

3.6.4 WiFi Protected Setup

In questa sezione è possibile configurare tutti i dettagli relativi alla funzionalità WiFi Protected Setup.
Questo insieme di specifiche, se supportate dai client collegati al dispositivo, permettono di semplificare l'associazione e la messa in sicurezza degli stessi.

Wi-Fi Protected Setup

WPS

WPS : Enabled Disabled Apply

Status : UnConfigured Configured

Self-PIN Number : 47361287

Client PIN Number

Start PIN

Push Button Configuration

Start PBC

Authentication	Encryption	Key
WPA2AUTO-PSK	TKIP	andrea08101984

WPS: Selezionare Enabled per attivare il supporto WPS del dispositivo o Disable per non utilizzare questa funzionalità.
Status: Indica lo stato del supporto.
Self-PIN Number: Visualizza il codice PIN identificativo per il dispositivo.

Le specifiche Wifi Protected Setup permettono l'utilizzo di 2 modalità: PIN Mode e PBC Mode.
Di seguito sono riportate le configurazioni necessarie per ognuna delle opzioni.

PIN MODE

In questa modalità di connessione, l'associazione dei client e la configurazione dei parametri di connessione della rete wireless vengono gestite tramite l'immissione di un codice numerico (PIN) assegnato al client e alla BSE.
Per associare un client al dispositivo tramite la modalità PIN, seguire la seguente procedura:

1. Accedere all'utility di configurazione del client (A02-UP-W300N o A02-PCI-W300N) e annotare il codice PIN visualizzato nel campo **Pin Code**.
2. Inserire il codice annotato nel campo relativo sulla pagina di configurazione del WebShare e premere il pulsante **Start PIN** per avviare la modalità di sincronizzazione.
3. Premere il pulsante **PIN** sull'utility del client per avviare il processo di sincronizzazione.

La barra di progresso indicherà, in maniera percentuale, lo stato di esecuzione della sincronizzazione.

PBC MODE

In questa modalità di connessione, l'associazione dei client e la configurazione dei parametri di connessione della rete wireless vengono gestite la pressione di un tasto (fisico o virtuale).
Per associare un client al dispositivo tramite la modalità PBC, seguire la seguente procedura:

1. Premere il pulsante WPS posto sul lato destro del prodotto (vista frontale); lo stesso indicherà l'attivazione della modalità di sincronizzazione tramite un lampeggio regolare del pulsante.
2. Accedere all'utility di configurazione del client (A02-UP-W300N o A02-PCI-W300N) e verificare la presenza dell' SSID del prodotto sotto la voce WPS -> WPS AP List.
3. Premere il pulsante PCB sull'utiliy per avviare la sincronizzazione del client con il WebShare RB300.

La barra di progresso indicherà, in maniera percentuale, lo stato di esecuzione della sincronizzazione.

3.7 LAN

3.7.1 Basic

Questa sezione permette la configurazione dei parametri relativi all'interfaccia LAN del dispositivo.

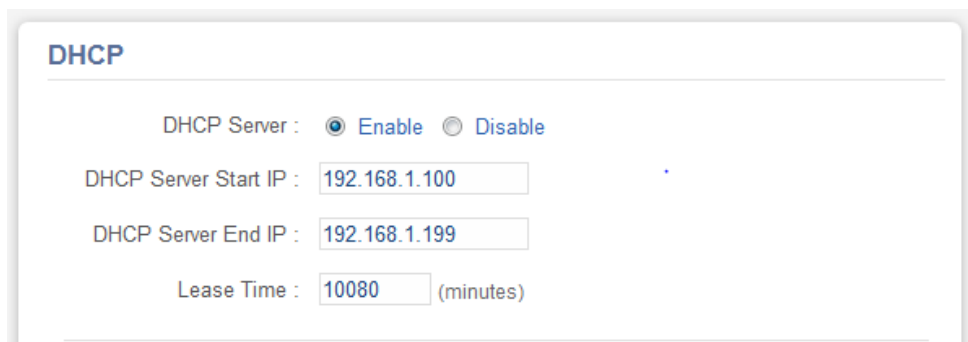
Basic

Host Name : Wireless Router

IP Address : 192.168.1.1

Subnet Mask : 255.255.255.0

Cancel Apply

Host Name: Inserire il nome del dispositivo.
IP Address/Subnet Mask: Questo è l'indirizzo IP con cui il Wireless Broadband Router è visto nella LAN (potrebbe essere un IP pubblico nel caso l'ISP fornisca una classe pubblica routata). E' necessario, qualora si cambiasse IP con quello di un'altra subnet accertarsi che tutti i PC della LAN abbiano un indirizzo IP (se non sono settati come client DHCP) nella stessa subnet. Diversamente questo potrebbe impedire il corretto funzionamento della LAN e l'accesso al Router.

Cliccare su **Apply** per salvare le modifiche.

Nel caso in cui l'IP del prodotto venga impostato su una classe di rete differente (es: 192.168.2.1), il DHCP provvederà ad adeguarsi alla nuova rete in maniera automatica.

3.7.2 DHCP

In questa sezione è possibile configurare i settaggi del DHCP Server integrato nel Wireless Broadband Router.

DHCP

DHCP Server : Enable Disable

DHCP Server Start IP : 192.168.1.100

DHCP Server End IP : 192.168.1.199

Lease Time : 10080 (minutes)

DHCP Server: Sono disponibili 2 differenti opzioni:

- **Disable:** Selezionare per NON usare il DHCP Server nel Router che dunque non distribuirà gli indirizzi IP ai vari clients DHCP. In questo caso bisogna assegnare manualmente a tutti i PC della rete un indirizzo IP (diverso per ogni PC), la subnet mask, DNS e l'indirizzo del gateway (che,dovrebbe essere quello del Wireless Broadband Router nel caso sia usato in modalità Router, oppure del Router ADSL/ISDN nel caso in cui sia usato in modalità Access Point).
- **Enable:** Selezionare per usare il DHCP Server nel Router che dunque distribuirà gli indirizzi IP, subnet mask, gateway (l'indirizzo IP del Router) e DNS ai vari clients DHCP.

DHCP Server Start IP: Introdurre l'indirizzo IP di partenza del pool che il server DHCP assegnerà ai vari client. Il valore di default è: 192.168.1.100.

DHCP Server End IP: Introdurre l'indirizzo IP finale del pool che il server DHCP assegnerà ai vari client. Il valore di default è: 192.168.1.199.

Lease Time: Immettere il termine di scadenza scadenza dell'associazione IP fornita dal DHCP; al termine della stessa, il DHCP provvederà al rinnovo dell'IP associato al client.

Static DHCP: Selezionare **Enable** nel caso in cui sia necessario associare in maniera statica un indirizzo IP ad un determinato MAC.

Name: Inserire il nome di identificazione dell'associazione statica che si sta immettendo.

MAC Address: Inserire il MAC Address al quale verrà associato staticamente l'indirizzo IP che verrà specificato nel campo **IP Address.**

IP Address: Inserire l'IP da associare staticamente al MAC Address specificato nel campo **MAC Address**.

Add Static DHCP

Static DHCP : Enable Disable

Name :

MAC address : - - - - -

IP address :

Nelle tabelle **Static DHCP List** e **Dynamic DHCP List** è possibile verificare le associazioni, statiche e dinamiche, del DHCP Server.
Nella tabella **Dynamic DHCP List** sarà quindi possibile visualizzare i client connessi al Wireless Broadband Router, mentre le associazioni presenti nella **Static DHCP List** rimarranno visibili anche se il client interessato non è connesso al prodotto.

Static DHCP List

Host Name	MAC Address	IP Address	

Dynamic DHCP List

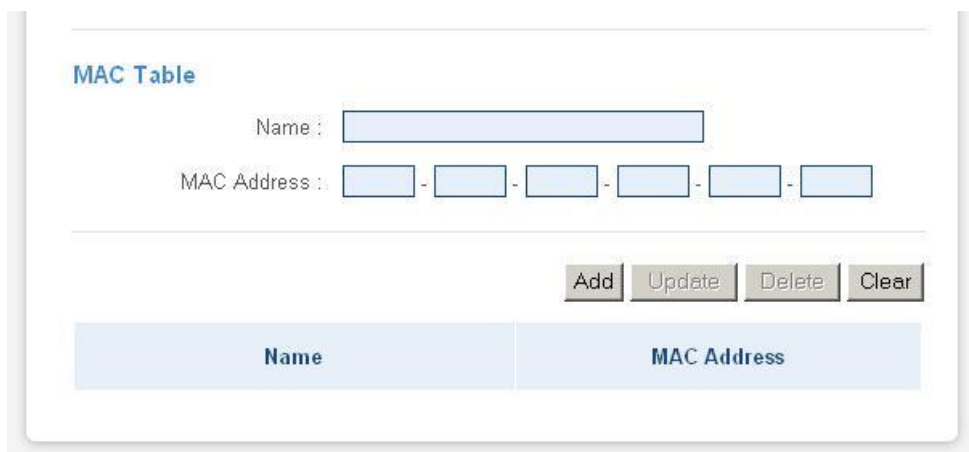
Host Name	MAC Address	IP Address	Expired Time
unknown	00-e0-18-df-7b-64	192.168.1.127	Apr/08/2002 00:00:00

3.8 Access Control

Questa sezione contiene i settaggi relativi al NAT e al Firewall del Wireless Broadband Router.

3.8.1 Filter

In questa sezione è possibile configurare diversi tipi di filtraggio sul traffico proveniente dalla LAN verso l’interfaccia WAN.

MAC FILTER

Quesa sezione permette di configurare il Wireless Broadband Router in modo da fornire l’accesso solo dopo aver controllato il MAC address del client wireless.
E’ possibile pertanto permettere:

- l’accesso ad una lista esclusiva di MAC address (selezionare **Only allow computers with MAC address listed below to access the network**)
- l’accesso a tutti e bloccare una lista di MAC address ben precisa (selezionare **Only deny computers with MAC address listed below to access the network**)

Dopo aver selezionato la politica da attuare, cliccare sul tast **Apply** per salvare le modifiche.
Ora sarà necessario inserire una lista di indirizzi MAC da bloccare o a cui permettere l’accesso.

Name: Introdurre un nome identificativo per la regola immessa.
***MAC Address**:* Introdurre l’indirizzo MAC da inserire nella lista.

Premere il pulsante **Add** per aggiungere il MAC immesso alla lista dei MAC Address da permettere/inibire.
Premere il pulsante **Delete**, dopo aver selezionato un entry per eliminarla oppure il tasto **Update** per aggiornare le informazioni relative alla regola selezionata dopo una modifica.

PROTOCOL/IP FILTER
In questa sezione è possibile impostare delle regole di filtraggio utilizzando come criterio di selezione l'indirizzamento IP o il protocollo di comunicazione.

Edit Protocol/IP Filter in List

Enabled : Enable Disabled

Name :

Protocol : TCP

Port : -

IP Range : -

Add Update Delete Clear

	Name	Protocol	Port	IP Range
	Filter FTP	Any	20-21	0.0.0.0-0.0.0.0
	Filter HTTP	Any	80-80	0.0.0.0-0.0.0.0
	Filter HTTPS	Any	443-443	0.0.0.0-0.0.0.0
	Filter DNS	Any	53-53	0.0.0.0-0.0.0.0
	Filter SMTP	Any	25-25	0.0.0.0-0.0.0.0
	Filter POP3	Any	110-110	0.0.0.0-0.0.0.0
	Filter Telnet	Any	23-23	0.0.0.0-0.0.0.0

Enable/Disable: Abilita o disabilita il filtraggio per indirizzo IP.
Name: Inserire il nome d assegnare alla regola di filtraggio.

Protocol: Selezionare il tipo di protocollo tra TCP, UDP o *.
Port: Immettere il numero di porta o il range di porte da filtrare.
IP Range: Inserire rispettivamente il primo e l'ultimo indirizzo IP da filtrare. (nel caso si tratti di un IP singolo, sarà necessario riportare lo stesso indirizzo IP in entrambi i campi).

Premere il pulsante **Add** per aggiungere il MAC immesso alla lista dei MAC Address da permettere/inibire.
Premere il pulsante **Delete**, dopo aver selezionato un entry per eliminarla oppure il tasto **Update** per aggiornare le informazioni relative alla regola selezionata dopo una modifica.

DOMAINS/URL BLOCKING
Quesa sezione permette di configurare il Wireless Broadband Router in modo da fornire/inibire la navigazione su alcuni siti/domini. E' possibile pertanto permettere:

- l'accesso ad una lista esclusiva di domini (selezionare **Allow users to access all domains list**)
- il blocco dell'accesso ad una lista di domini (selezionare **Allow users to access all domains list**)

Dopo aver selezionato la politica da attuare, cliccare sul tast **Apply** per salvare le modifiche.
Ora sarà necessario inserire i domini da inserire nella lista da bloccare o a cui permettere l'accesso.

Domains/URL List

Block those URLs which contain keywords listed below.

Delete

Add Cancel

3.8.2 Virtual Server

Il Firewall/Nat del Wireless BroadBand Router consente la protezione della LAN locale da parte di accessi indesiderati. Può essere necessario, consentire ad utenti esterni l'accesso ad un PC specifico della Lan (per esempio verso un PC fa da server Web o FTP). La funzionalità di Virtual Server consente di reindirizzare un particolare servizio, che avviene su una determinata porta (si ricorda che Web =80, FTP =20/21, Telnet =23, SMTP =25, POP3 =110, DNS =53, ECHO =7, NNTP =119) , su un PC della Lan interna. E' possibile scegliere la porta ed il protocollo (tra TCP,UDP o entrambi) che si intende rigirare sull'indirizzo IP.

Virtual Server

Enabled : Enabled Disabled

Name :

Protocol : TCP

Private Port :

Public Port :

LAN Server :

Add Update Delete Clear

Enabled: Abilita o disabilita la funzionalità la regola selezionata o che si sta creando.
Name: Inserire il nome identificativo della regola che si sta creando o che si selezionato dall'elenco di regole preconfigurate.
Protocol: Selezionare il tipo di protocollo (scegliere tra TCP, UDP o entrambi)
Private Port: Inserire il numero di porta (compreso tra 0-65535)
Public Port: Inserire il numero di porta (compreso tra 0-65535)
LAN Server: Inserire l'indirizzo IP su cui è necessario reindirizzare il servizio.

La sezione Firewall viene prima di quella del Virtual Server, assicurarsi che le porte/protocolli ruotati non siano bloccati dal Firewall.

Sono inoltre presenti tutta una serie di Virtual Server preconfigurati, come da figura:

Add Update Delete Clear

	Name	Protocol	LAN Server
☐	Virtual Server FTP	TCP 21/21	0.0.0.0
☐	Virtual Server HTTP	TCP 80/80	0.0.0.0
☐	Virtual Server HTTPS	TCP 443/443	0.0.0.0
☐	Virtual Server DNS	UDP 53/53	0.0.0.0
☐	Virtual Server SMTP	TCP 25/25	0.0.0.0
☐	Virtual Server POP3	TCP 110/110	0.0.0.0
☐	Virtual Server Telnet	TCP 23/23	0.0.0.0
☐	IPSec	UDP 500/500	0.0.0.0
☐	PPTP	TCP 1723/1723	0.0.0.0
☐	NetMeeting	TCP 1720/1720	0.0.0.0

Se sul Wireless Broadband Router è abilitato il DHCP bisogna prestare particolare attenzione ad assegnare l'indirizzo IP dei Virtual Server per evitare conflitti. In questo caso è sufficiente assegnare al Virtual Server (Tale PC non sarà client DHCP ed avrà oltre all'indirizzo IP, la subnet mask, il gateway (cioè l'IP privato del Wireless Broadband Router) ed i server DNS) un indirizzo IP che sia nella stessa subnet del Router ma fuori dal range di indirizzi IP assegnabili dal server DHCP attivo sul Router.

Se per esempio il server WEB (che riceverà chiamate sulla porta 80) della LAN ha indirizzo IP privato 192.168.1.127 anzitutto è necessario evidenziare nella

tabella il servizio opportuno. Poi abilitarlo (spuntando **enable**, configurarlo mettendo l'IP 192.168.1.2 ed infine validarlo premendo **update**). Il risultato finale dovrebbe essere come in figura sotto.

E' chiaro che in questo caso non dovremo utilizzare il DHCP client sul PC poichè in tal caso non conosceremo l'IP che il server Web potrebbe prendere.

E' importante sapere che il Wireless Broadband Router esegue, in ordine di numerazione crescente, le associazioni richieste dai vari Virtual Server e solo alla fine (qualora fosse presente) rigira il tutto alla DMZ. Pertanto se la porta (20)21 è mappata (ad esempio) su un certo PC della rete tramite Virtual Server, il PC il cui indirizzo è indicato nel DMZ non potrà funzionare come server FTP.

Alcune applicazioni Internet ormai oggi diffusissime necessitano, per essere usate pienamente, di una configurazione particolare della sezione Virtual Server del Router. Nella lista seguente sono presenti questi settaggi. La lista non vuole essere esaustiva ma solo un punto d'inizio, invitiamo a consulare eventuali aggiornamenti di questo manuale.

Applicazione	Settaggi connessioni Uscenti	Settaggi connessioni Entranti
ICQ 98, 99a	Nessuno	Nessuno
NetMeeting 2.1 a 3.01	Nessuno	1503 TCP, 1720 TCP
VDO Live	Nessuno	Nessuno
MIRC	Nessuno	Nessuno
Cu-SeeMe	7648 TCP &UDP, 24032 UDP	7648 TCP &UDP, 24032 UDP
PC AnyWhere	5632 UDP, 22 UDP, 5631 TCP, 65301 TCP	5632 UDP, 22 UDP, 5631 TCP, 65301 TCP
Edonkey	Nessuno	principalmente 4660-4662 TCP , 4665 UDP
MSN Messanger	Nessuno	TCP da 6891-6900 TCP 1863 TCP 6901 UDP 1863, 6901 e 5190

Usando NetMeeting (Versione3.0), ad esempio, quando la chiamata generata è uscente da un PC dietro al Router verso un PC esterno non ci sono problemi. Il contrario non è realizzabile. Rigirando invece le porte 1503(TCP) e 1720(TCP) è

possibile ricevere anche chiamate in ingresso con video (h.323 e T.120). In figura è presente una configurazione di VS per ricevere chiamate in ingresso in Netmeeting (vengono rigirate al PC con IP 192.168.2.100).

Attenzione il Router può gestire un numero non infinito di connessioni entranti, pertanto per grandi range (o centinaia di connessioni contemporanee) potrebbero sorgere problemi derivanti dal limite fisico della memoria allocabile dal processo NAT.

Sono allegate tutta una serie di porte notevoli (da utilizzarsi per il VS ed il Firewall):

Servizio	Numero di Porta / Protocollo
File Transfer Protocol (FTP) Data	20/tcp
FTP Commands	21/tcp
Telnet	23/tcp
Simple Mail Transfer Protocol (SMTP) Email	25/tcp
Domain Name Server (DNS)	53/tcp and 53/udp
Trivial File Transfer Protocol (TFTP)	69/udp
finger	79/tcp
World Wide Web (HTTP)	80/tcp
POP3 Email	110/tcp
SUN Remote Procedure Call (RPC)	111/udp
Network News Transfer Protocol (NNTP)	119/tcp
Network Time Protocol (NTP)	123/tcp and 123/udp
News	144/tcp
Simple Management Network Protocol (SNMP)	161/udp
SNMP (traps)	162/udp
Border Gateway Protocol (BGP)	179/tcp
Secure HTTP (HTTPS)	443/tcp
rlogin	513/tcp
rexec	514/tcp
talk	517/tcp and 517/udp
ntalk	518/tcp and 518/udp
Open Windows	2000/tcp and 2000/udp
Network File System (NFS)	2049/tcp
X11	6000/tcp and 6000/udp
Routing Information Protocol (RIP)	520/udp
Layer 2 Tunnelling Protocol (L2TP)	1701/udp

3.8.3 Special AP

E’ possibile abilitare particolari applicazioni, come i videgames, che richiedono connessioni multiple (generalmente critiche quando si usa il NAT). Sono già contenuti tutta una serie di settaggi per i videogames/applicazioni più comuni.

Special AP

Enabled : (•) Enabled ( ) Disabled
Name : Battle.net

Trigger
Protocol : *
Port Range : 6112 - 6112

Incoming
Protocol : *
Port : 6112

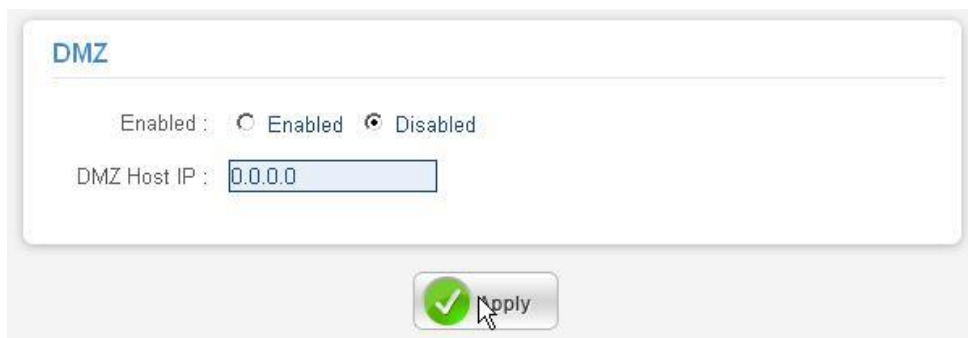
Add | Update | Delete | Clear

	Name	Trigger	Incoming
☐	Battle.net	* 6112	* 6112

Name: Tipo descrittivo dell’applicazione.
Trigger: Definisce le porte e protocolli delle comunicazioni uscenti che determinano poi le porte ed i protocolli di comunicazioni entranti.

- **Protocol:** Selezionare tra TCP, UDP oppure ICMP.
- **Port Range**: Selezionare l’intervallo di porte usato dall’applicazione

Incoming: Definisce l’intervallo di porte da aprire in risposta alla comunicazione uscente.

- **Protocol:** Selezionare l'intervallo di porte usato dall'applicazione.
- **Port:** Selezionare l'intervallo di porte usato dall'applicazione.

Premere il pulsante **Add** per aggiungere il MAC immesso alla lista dei MAC Address da permettere/inibire.
Premere il pulsante **Delete**, dopo aver selezionato un entry per eliminarla oppure il tasto **Update** per aggiornare le informazioni relative alla regola selezionata dopo una modifica.

E' possibile, selezionare dalla lista già presente, abilitare/disabilitare il servizio e poi premere su **Update**.

3.8.4 DMZ

E' a tutti gli effetti un computer esposto ad Internet, un pacchetto in ingresso viene esaminato dal Firewall (passa il NAT) e passato all'indirizzo contenuto nel DMZ (se non soddisfa un Virtual Server).

DMZ

Enabled : Enabled Disabled

DMZ Host IP : 0.0.0.0

Apply

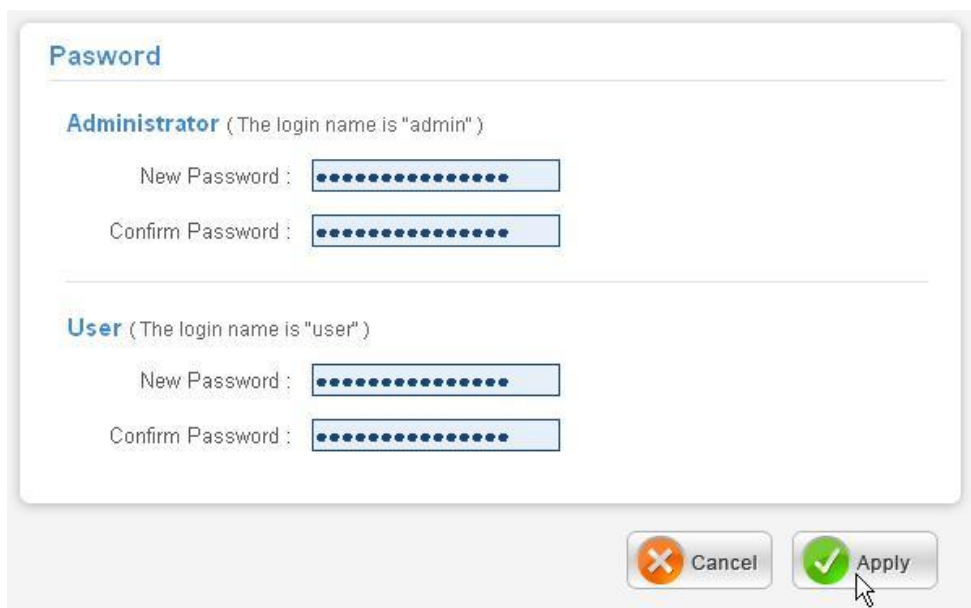
Enabled: Per abilitare la funzionalità DMZ.
DMZ Host IP: Indicare l'indirizzo IP della macchina sulla quale verrà indirizzato tutto il traffico entrante.

Cliccare su **Apply** per salvare le modifiche.

In questo modo l'indirizzo IP è completamente esposto.

3.8.5 Firewall Settings

Questa sezione permette di configurare la policy di filtraggio del traffico in base a 3 differenti modalita.

Endpoint Independent: Il traffico in ingresso, indirizzato verso una porta aperta, verrà inoltrato all'applicazione che ha richiesto l'apertura di tale porta.
Address Restricted: L'indirizzo di destinazione del traffico entrante deve corrispondere all'indirizzo IP della connessione in uscita.
Address And Port Restriction: L'indirizzo e la porta di destinazione del traffico entrante devono corrispondere all'indirizzo IP ed alla porta comunicazione della connessione in uscita.

3.9 System

3.9.1 Password

In questa sezione è possibile configurare le password di accesso dell'apparato. E' estremamente importante sostituire la password di accesso al Wireless Broadband Router per incrementare il livello di sicurezza del dispositivo.
In questa sezione sarà possibile reimpostare la password di amministratore (admin) e quella utente (user).

Introdurre la nuova password in **New Password** e poi per conferma in **Confirm Password.** La password può essere composta al massimo da 16 caratteri alfanumerici.

Pasword

Administrator (The login name is "admin")

New Password : ●●●●●●●●●●●●●●●

Confirm Password : ●●●●●●●●●●●●●●●

User (The login name is "user")

New Password : ●●●●●●●●●●●●●●●

Confirm Password : ●●●●●●●●●●●●●●●

Cancel Apply

Cliccare poi su **Apply** per rendere operativa la nuova password di accesso.

E' possibile, qualora si dimenticasse la password di accesso del dispositivo, resettarlo premendo l'apposito bottone (per almeno 10 secondi) posto sul retro. A questo punto verrà caricato il firmware con le impostazioni di default (username=**admin**, password=**admin**).

3.9.2 Time

Il Router non ha un orologio al suo interno, usa il protocollo SNTP per risolvere tale inconveniente.

Local Time: Viene mostrata l'ora

Time Zone: Per scegliere la zona di appartenenza sarà sufficiente selezionare il fuso di appropriato; selezionare poi **Enable** sul campo Synchronize the Clcck with NTP Server ed inserire l'indirizzo di un server NTP nel campo NTP Server.
NTP Server: Introdurre l'indirizzo IP del server opportuno.

MANUALLY DATE AND TIME SETTING
Per introdurre manualmente l'ora. Cliccare poi su **Set Time** per salvare le nuove impostazioni orarie.

DAYLIGHT SAVING
Scegliere **Enable** e immettere il periodo entro cui è attiva l'ora legale.

Cliccare poi su **Apply** per salvare le modifiche.

3.9.3 Device Information

In questa sezione è possibile conoscere i dettagli relativi all'interfaccia WAN, LAN e WLAN. La sezione è suddivisa in **WAN**, **Wireless**, **LAN** e **DHCP Client List**..

WAN
Visualizza tutti i parametri relativi all'interfaccia WAN.

Device Information
WAN
MAC Address : 00-18-e7-11-44-73
Connection Type : DHCP Client Disconnected
DHCP Release
DHCP Renew
IP Address : 0.0.0.0
Subnet Mask : 0.0.0.0
Default Gateway : 0.0.0.0
DNS :

WIRELESS
Visualizza tutti i parametri relativi all'interfaccia WLAN

Wireless

Connection : 802.11g AP Enable
SSID : default
Channel : 6
Antenna Power : Full
Authentication Type : Disabled
Wireless Client List :

LAN
Visualizza tutti i parametri relativi all'interfaccia LAN.

LAN

MAC Address : 00-18-e7-11-44-72
IP Address : 192.168.1.1
Subnet Mask : 255.255.255.0
DHCP Server : Enabled DHCP Client List

Connected Time	MAC Address	Mode

Nella sezione **DCHP Client List** sarà possibile visualizzare una lista dei client che sono associati al Wireless Broadband Router e che hanno fatto richiesta al DHCP Server integrato del prodotto.

3.9.4 Log

Il Router mostra tutti gli ultimi 200 Log (i più vecchi saranno sovrascritti dai più recenti).
Cliccando nei bottoni, nella parte superiore, è possibile rapidamente fare scorrere tutte le pagine dei vari log. Con **Clear Log** la memoria dei Log verrà cancellata e con **Refresh** è possibile ottenere un aggiornamento istantaneo.

3.9.5 Log Settings

E’ possibile configurare tutti i parametri relativi alla gestione dei Log.

Log Setting

SMTP Authentication : Enabled Disabled

SMTP Account :

SMTP Password :

SMTP Server :

From Email Address :

To Email Address :

Email Log Now

Log Type

System Activity

Debug Information

Attacks

Dropped Packets

Notice

Cancel Apply

SMTP Authentication: Scegliere **Enabled** per utilizzare la funzione di segnalazione via email.

SMTP Account: Introdurre l’account per l’autenticazione sul server SMTP dell’ISP affinché il Router possa inviare all’indirizzo mail, contenuto nel campo **To Email Address**, tutti i dettagli relativi ai Log.

SMTP Password: Introdurre la password per l'autenticazione sul server SMTP dell'ISP dell'account inserito nel campo **SMTP Account**.
SMTP Server: Introdurre il nome o l'indirizzo IP del server SMTP da utilizzare.
From Email Address: Introdurre l'indirizzo mail con cui inviare i Log.
To Email Address: Introdurre l'indirizzo mail cui inviare i Log. Cliccando su **Email Log Now** effettuerete un invio immediato.

LOG TYPE
Selezionare i contenuti del Log:

- **System Activity:** Mostra le informazioni relative all'attività dell'apparato.
- **Debug Information:** Mostra le informazioni circa il corretto caricamento dei moduli dell'apparato.
- **Attacks:** Mostra informazioni circa qualsiasi attività sospetta.
- **Dropped Packets:** Mostra informazioni sui pacchetti che non sono trasferiti con successo.
- **Notice:** Notizie riservate all'amministratore

Cliccare poi su **Apply** per salvare le modifiche.

3.9.6 Statistics

In questa sezione è possibile conoscere i dettagli relativi all'interfaccia WLAN e WAN. Vengono mostrate le informazioni relative al numero di pacchetti spostati.

Statistic

TUtilization (bytes/sec)		LAN	WAN	Wireless
Send	Average :	16	0	1
	Peak :	120	0	1
Receive	Average :	27	0	0
	Peak :	171	0	0

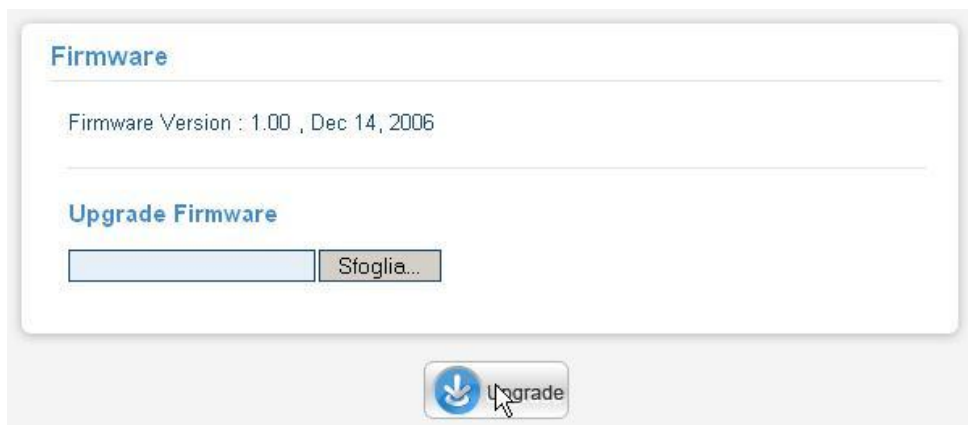
Reset

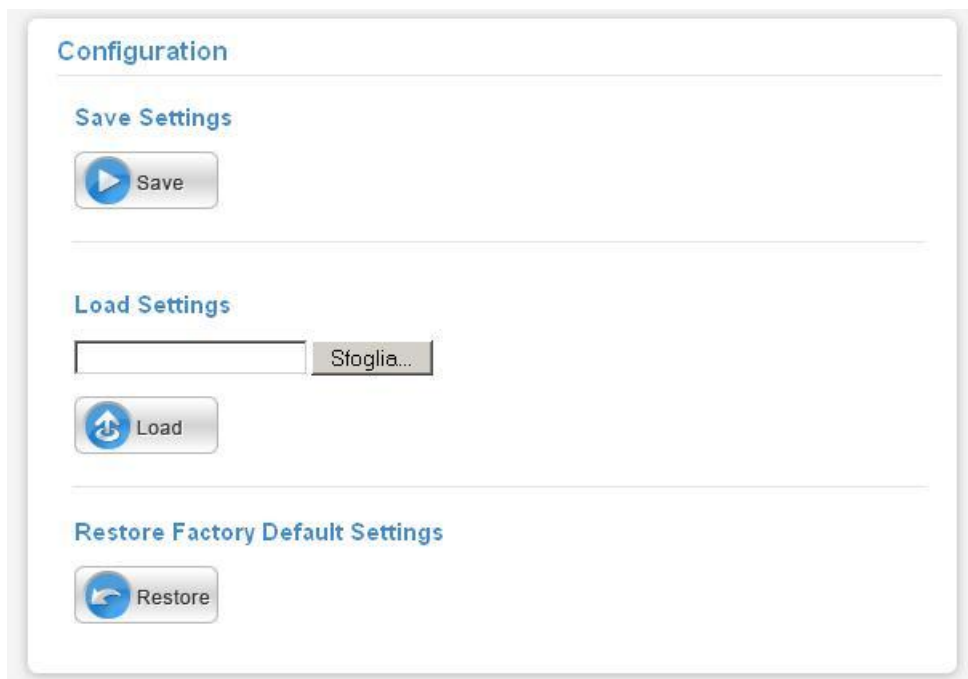
Cliccare su **Reset** per azzerare le statistiche.

3.9.7 Restart

Premere sul pulsante Restart per riavviare il prodotto mantenendo le configurazioni salvate.

3.9.8 Firmware

In questa sezione è possibili visualizzare la versione di firmware caricata sul Wireless Broadband Router ed effettuare l’aggiornamento dello stesso.

Firmware Version: Mostra la versione di firmware correntemente utilizzata dal Wireless Broadband Router.
Upgrade Firmware: E’ possibile effettuare l’upgrade del firmware del dispositivo. Seguire le seguenti istruzioni :

- Scaricare l’ultimo firmware dal sito www.atlantis-land.com
- Cliccare sul bottone **Sfoglia**, indicando il percorso dove è contenuto il file precedentemente scaricato, e cliccare poi su **Upgrade**.

E’ opportuno garantire, durante l’intera fase di upgrade, al Wireless Broadband Router l’alimentazione elettrica. Qualora questa venisse a mancare il dispositivo potrebbe non essere recuperabile.
Staccare il cavo WAN dal Router.
Non effettuare upgrade del firmare utilizzando l’interfaccia wireless ma solo quella wired. Questo potrebbe danneggiare il dispositivo ed invalidare la garanzia.

3.9.9 Configuration

Il Wireless Broadband Router consente di effettuare un backup (ripristino) sul (dal) disco fisso del vostro PC. Grazie a questa comoda funzionalità è possibile salvare complesse configurazioni e rendere nuovamente operativo il Router in pochi veloci passaggi.

Configuration

Save Settings

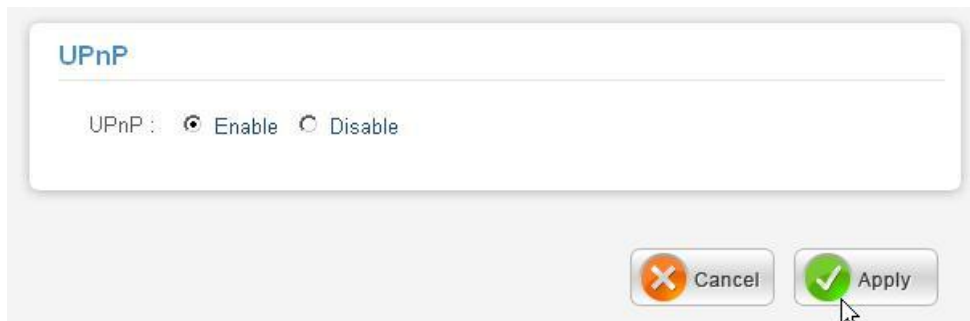
Save

Load Settings

Sfoglia...

Load

Restore Factory Default Settings

Restore

Per effettuare il Backup cliccare sul bottone **Save (in Save Settings)**. Non resta che selezionare il percorso in cui salvare i dati sulla configurazione (verrà generato un file config.BIN).
Per effettuare il Ripristino cliccare sul bottone **Sfoglia**, indicando il percorso dove è contenuto il file contenente la configurazione, e cliccare poi su **Load.**
Se per necessità si desidera reimpostare il router Wireless con la configurazione di default (perdendo tutti i settaggi inseriti) sarà sufficiente premere poi il tasto **Restore**. Il Router effettuerà un reboot e caricherà i settaggi di default.

3.9.10 UPnP

Il Wireless Broadband Router è dotato di un supporto UpnP, al fine di garantire il più alto grado di compatibilità con qualsiasi software.

Selezionare la voce **Enable** per abilitare questa funzionalità, e premere su **Apply** per confermare l'operazione.

3.9.11 Ping Test

Il Wireless Broadband Router è dotato di un utility in grado di effettuare un ping test verso un indirizzo IP (o un host) specificato, al fine di verificare la connettività del prodotto.

Inserire l'indirizzo IP o l'Host Name verso cui effettuare una Echo Request.
Cliccare poi su **Ping** per effettuare l'operazione; verrà restituito l'esito del Ping Test.

3.9.12 Remote Management

In queste sezioni è possibile configurare le modalità con cui il dispositivo viene controllato da remoto.

HTTP: Consente l'accesso HTTP da remoto.

- **Enable:** per abilitare tale funzionalità
- **Port:** permette di scegliere la porta tramite cui configurare il dispositivo.
- **Remote IP Range:** consente di introdurre il range di IP da cui si effettua la configurazione remota.

Allow to PING WAN Port: Cliccando su **Enable**, consente di bloccare/permetter il ping sulla porta WAN.
PPTP: Spuntare questa funzione per abilitare la funzione di VPN PPTP Pass-Through.
L2TP: Spuntare questa funzione per abilitare la funzione di VPN PPTP Pass-Through.
IPSec: Spuntare questa funzione per abilitare la funzione di VPN IPSec Pass-Through.
IDENT: Permette all'utente di impostare la porta 113 in modalità Stealth..

APPENDICE A: Risoluzione dei problemi

Questo capitolo illustra come identificare e risolvere eventuali problemi sul Wireless Broadband Router.

A.1 LEDs

I LEDs sono un utile strumento per individuare eventuali problemi, osservandone lo stato è possibile individuare velocemente dove si verifica un eventuale malfunzionamento.

A.1.1 LED Power

Il LED PWR non si accende

Steps	Azione Correttiva
1	Accertarsi che l'alimentatore sia connesso al Wireless Broadband Router e alla rete elettrica. Utilizzare unicamente l'alimentatore fornito a corredo.
2	Verificare che l'alimentatore sia connesso ad una presa elettrica attiva e in grado di fornire la tensione necessaria al funzionamento del prodotto.
3	Accertarsi che il Plug dell'alimentatore sia correttamente inserito.
4	Se il problema persiste contattare l'assistenza tecnica Atlantis Land.

A.1.2 LED LAN

Il LED LAN non si accende.

Steps	Azione Correttiva
1	Verificare la connessione del cavo di rete tra il Wireless Broadband Router e il PC o lo Switch di rete.
2	Verificare che il cavo sia funzionante.
3	Verificare che la scheda di rete del PC funzioni correttamente.
4	Se il problema persiste contattare l'assistenza tecnica Atlantis Land.

A.1.3 LED WLAN

Il LED WLAN non si accende.

Steps	Azione Correttiva
1	Effettuare un reset ed attendere una cinquantina di secondi (tempo di reinizializzazione del modulo WLAN)
2	Eventualmente staccare il cavo di alimentazione e reinserirlo.

A.1.4 LED STATUS

Il LED STATUS non si accende o rimane acceso fisso.

Steps	Azione Correttiva
1	Staccare il cavo di alimentazione e reinserirlo.
2	E' possibile effettuare una procedura di recovery al fine di tentare il recupero dell'apparato. 1. Eseguire il download del recovery firmware dal sito www.atlantis-land.com o dalla cartella Recovery presente sul CD-Rom a corredo. 2. Premere il tasto di reset sulla parte posteriore del prodotto, mantenendo scollegata l'alimentazione. 3. Collegare il plug d'alimentazione mantenendo premuto il tasto di reset per circa 15 secondi. 4. Accedere all'indirizzo http://192.168.1.1 5. Selezionare il file con estensione .bin precedentemente scaricato e premere sul tasto Upload.

A.2 Configurazione WEB

Non è possible accedere all'interfaccia Web di configurazione.

Steps	Azione correttiva
1	Accertarsi di utilizzare un indirizzo IP corretto, appartenente alla stessa rete del Wireless Broadband Router (192.168.1.1).
2	Effettuare un reset del dispositivo.

Le schermate di configurazione Web non vengono visualizzate correttamente..

Steps	Azione correttiva
1	Accertarsi di utilizzare Internet Explorer 5 o una versione successiva.
2	Eliminare i files temporanei di Internet ed eseguire un nuovo login.

A.3 Login con Username e Password

E' stata dimenticata la password di accesso.

Steps	Azione correttiva
1	Se è stata cambiata la password di accesso ed è stata dimenticata, sarà necessario caricare la configurazione di default. Ciò cancellerà tutte le configurazioni eseguite dall'utente e ripristinerà la password di default. Premendo il pulsante "**Reset**" presente nel pannello posteriore del prodotto per una decina secondi, il Wireless Broadband Router riporterà tutte le impostazioni ai valori iniziali (il tasto WLAN si spegnerà per indicare l'avvenuto reset, ricomincerà poi il caricamento di tutti i moduli necessari al funzionamento dell'apparato).
2	I parametri di default per l'accesso alla configurazione del Wirless Broadband Router sono: **Username: admin** **Password: admin** **IP:192.168.1.1** **Canale=6** **Sicurezza=Disabilitata** **SSID=N Router**
3	Per incrementare il livello di sicurezza del sistema è molto importante modificare la password di default.

A.4 Amministrazione remota

Non è possibile amministrare il Wireless Broadband Router da remoto.

Steps	Azione correttiva
1	Assicurarsi di aver abilitato la funzionalità Remote Management.
2	Assicurarsi che l'IP della macchina da cui si effettua il controllo remoto sia nel range di IP permessi(Management-Remote Management).

A.5 Domande Generali

Domanda	Cosa è lo standard IEEE 802.11g ?
Risposta	Il nuovo standard 802.11g opera alla frequenza di 2,4 GHz e quindi è pienamente compatibile con la più diffusa versione b. Il vantaggio è che consente una velocità di trasferimento di 54 Mbps, cinque volte superiore allo standard 802.11b.

Domanda	Cosa è il draft 802.11n ?
Risposta	Il nuovo insieme di specifiche 802.11n opera sulla frequenza di 2,4 GHz e quindi è pienamente compatibile con le più diffuse versioni b/g. I principali vantaggi rispetto agli standard precedenti sono importanti incrementi in termini di velocità (fino a 300 Mbps) e in termini di copertura (fino a 10 volte più estesa). La tecnologia radio MIMO permette inoltre di poter sfruttare la trasmissione su cammini multipli per incrementare il throughput, rendendo il prodotto particolarmente adatto per infrastrutture indoor.

Domanda	Cosa è il Wi-Fi Protected Setup?
Risposta	Il Wi-FI Protected Setup (WPS) è un insieme di specifiche supportate dal prodotto in grado di permettere la messa in opera dell'infrastruttura wireless con un solo click. Per informazioni, è possibile consultare la documentazione pubblica messa a disposizione dalla WiFi Alliance al link: http://www.wi-fi.org/wifi-protected-setup

Domanda	Posso avviare un' applicazione da un computer remoto presente sulla rete wireless?
Risposta	Questo dipende direttamente dall'applicazione stessa, se è stata progettata per lavorare in rete (non fa differenza che sia wireless o cablata) non ci sarà alcun problema.

Domanda	Posso giocare in rete con gli altri computer presenti sulla WLAN?
Risposta	Si, se il gioco è dotato di funzionalità multiplayer in rete.

Domanda	Cos'è lo Spread Spectrum?
Risposta	La trasmissione Spread Spectrum si basa sulla dispersione dell'informazione su una banda molto più ampia di quella necessaria alla modulazione del segnale disponibile. Il vantaggio che si ottiene da questa tecnica di modulazione è infatti una bassa sensibilità ai disturbi radioelettrici anche per trasmissioni a potenza limitata. Questa caratteristica è ovviamente preziosa quando si devono trasmettere dei dati.

Domanda	Cosa sono DSSS e FHHS?
Risposta	DSSS (Direct-Sequence Spread-Spectrum): E' una particolare tecnologia di trasmissione per la banda larga che consente di trasmettere ogni bit in maniera ridondante. E' adatta in particolare per la trasmissione e la ricezione di segnali deboli. FHHS (Frequency Hopping Spread Spectrum): è una tecnologia che permette la condivisione tra più utenti di uno stesso insieme di frequenze. Per evitare interferenze tra periferiche dello stesso tipo le frequenze di trasmissione cambiano sino a 1.600 volte ogni secondo.

Domanda	Le informazioni inviate via wireless possono essere intercettate?
Risposta	Il Wireless Broadband Router offre funzionalità di crittografia WEP, WPA e WPA2 con crittografia in AES per garantire la massima sicurezza in termini di protezione dei dati..

Domanda	Cosa è il WPA?
Risposta	In attesa delle ratifica dello standard IEEE802.11i la Wi-Fi Alliance ha derivato dalla versione preliminare un insieme di specifiche che va sotto il nome di WPA (Wi-Fi Protected Access). Le caratteristiche peculiari del WPA sono: • Integrazione del TKIP (Temporal Key Integrity Protocol) per permettere il cambio della chiave e migliora il controllo di integrità dei pacchetti • Meccanismo avanzato per gestire l'autenticazione e il controllo degli accessi ai servizi di rete in modo centralizzato (802.11x tramite EAP, l'uso di TLS è obbligatorio)

	• La chiave di autenticazione è diversa da quella utilizzata per la cifratura (che grazie al TKIP cambia continuamente) • Permette l'autenticazione direttamente sull'AP (WPA-PSK) Tale protocollo è molto più robusto del WEP.

Domanda	Cosa è il WPA2?
Risposta	Approvato di recente dalla Wi-Fi Alliance, il nuovo standard WPA2 è l'evoluzione del primo WPA (Wi-Fi Protected Access) che è oggi supportato dalla maggior parte degli apparati compatibili IEEE802.11g. Lo standard WPA, richiesto prepotentemente dal mercato per porre fine alla debolezza intrinseca del WEP, ha purtroppo tratto dall'802.11i solo una parte delle specifiche. Il nuovo WPA2 invece abbracciando pienamente l'IEEE802.11i ha necessariamente introdotto il supporto per l'Advanced Encryption Standard (AES), protocollo di cifrature utilizzato già da tempo nelle VPN IPSec. I dispositivi WPA2 saranno compatibili con quelli WPA che però dovranno essere riaggiornati tramite il rilascio di nuovi firmware e/o driver. Il problema risiede nella capacità di calcolo (richiesta dall'AES) che rischierebbe di essere praticamente troppo elevata per gli apparati oggi in commercio. Il NetFly AP2-54M supporta già questo protocollo senza riduzione di performance.

Domanda	Che impatto hanno questio algoritmi di cifratura sulle performance?
Risposta	Nessuno. Il chipset garantisce infine il pieno supporto hardware, senza nessuna degradazione di performance, degli standard di sicurezza più recenti, come il Wi-Fi Protected Access (WPA/WPA2) ed IEEE802.11i.

Domanda	Cosa è la modalità Infrastructure?
Risposta	Nella configurazione Infrastructure una rete WLAN e una rete WAN comunicano tra loro tramite un access point e/o Wireless Broadband Router.

Domanda	Cosa è il Roaming?
Risposta	Il Roaming è la capacità di un utente che possiede un computer portatile di comunicare senza interruzioni mentre si muove liberamente all'interno di una rete wireless la cui estensione è stata incrementata grazie all'utilizzo di più access point.

Domanda	Cosa è la banda ISM?
Risposta	Questa frequenza è stata messa a disposizione dalla FCC, su richiesta delle aziende che intendevano sviluppare soluzioni wireless per l'uso civile quotidiano ed è generalmente contraddistinta dalla sigla ISM band (Industrial, Scientific and Medical). In questa frequenza operano solo dispositivi industriali, scientifici e medici a basse potenze.

Domanda	I client 802.11n funzionano con AP IEEE802.11b/g?
Risposta	Senza alcun dubbio è possibile utilizzare client 802.11n (draft) con AP IEEE802.11b/g. In questo caso si crea una WLAN ibrida. Le prestazioni ottenibili dai client 802.11n risultano essere di gran lunga peggiori in una rete ibrida che non in una WLAN con solo apparati 802.11n (draft). Il consiglio è quello di migrare l'intera WLAN verso client 802.11n, come A02-UP-W300N e/o A02-PCI-W300N.

Domanda	Come posso eliminare le interferenze che deteriorano le prestazioni della WLAN?
Risposta	Anzitutto spegnere (o allontanare) ogni dispositivo che operi nelle stesse frequenze. Utilizzare antenne direzionali per far "imbarcare" meno rumore ai dispositivi. In caso si altri AP adiacenti consultare la faq sull'assegnazione dei canali.

Domanda	Caratteristiche dell'Antenna?
Risposta	Scegliere attentamente l'antenna adatta alle proprie esigenze, rivolgendosi a personale qualificato richiedendo: • connettore tipo Reverse SMA, • compatibile con 802.11 standard (2.4Ghz) • 50 Omh di impedenza

	Si invita al rispetto delle normative vigenti (20dBm max)

Domanda	Cos'è la ricezione in Diversity?
Risposta	La propagazione elettromagnetica in un ambiente chiuso (o indoor) genera innumerevoli riflessioni dovute a cambiamenti di densità nel materiale attraversato. Queste riflessioni possono generare, soprattutto in ambienti interni pericolosi fenomeni: • Cammini multipli:dovuti all'arrivo (sul ricevitore ad esempio)di segnali diretti e riflessi. • Forti attenuazioni:dovuti all'attraversamento di materiali diversi Questo fenomeno è controllabile utilizzando antenne direttive o utilizzando 2 antenne in ricezione (cosiddetta diversity). Quando il dispositivo ricevente è colpito dal segnale controlla quale delle 2 antenne stia ricevendo il miglior rapporto segnale/rumore e utilizza quest'ultima. Si utilizzano in sostanza 2 punti spaziali diversi per effettuare un miglior campionamento del segnale ricevuto.

Domanda	Introduzione ai decibel (cos'è)?
Risposta	Il deciBel è un'unita misura relativa che esprime un rapporto fra 2 valori. E' importante sottolineare che è adimensionale (non si misura in watt) e permette di capire immediatamente lo scostamento dalla misura campione o riferimento. E' utilizzato perché permette di avere un'immediata percezione della differenza di 2 misurazioni, essendo il logaritmo una misura compressa e non lineare. L'equazione canonica è la seguente: dB = 10 log10 (P 2 / P 1). Dove P1 è la misura riferimento e P 2 è la misura istantanea.

Domanda	Introduzione al dBm (cos'è)?
Risposta	Definiamo il dBm=10 log 10 (P 2 / P 1), dove P1 =1 milliWatt (mW). E' possibile pertanto parlare di potenza trasmessa sia utilizzando il watt che il dBm. Nella tabella seguente è riportata l'equivalenza per i valori più

comuni (utilizzare la formula di sopra per valori non in tabella):

dBm	Watt	note
0	1 mW	
3	2 mW	
6	4 mW	
9	8 mW	
10	10 mW	
12	15,8 mW	
13	20 mW	
14	25 mW	
15	32 mW	
16	40 mW	
17	50 mW	
18	63 mW	
19	79 mW	
20	100 mW	Massima Potenza utilizzabile per WLAN a 2.4Ghz
23	200 mW	
26	400 mW	
29	800 mW	

Domanda Cos' è un'antenna Isotropica?

Risposta Antenna che irraggia senza prediligere alcuna specifica direzione nello spazio circostante. E' possibile fare un paragone con l'irraggiamento luminoso di una lampadina che avviene uniformemente in tutto lo spazio circostante.
Effettuando una rilevazione della densità superficiale di potenza su una superficie sferica, il cui centro è posto sull'antenna, questa è uniforme.
Tale valore, espresso in [W]/[m^2], è legato all'inverso del quadrato della distanza tra il punto in cui si effettua la rilevazione e la sorgente (punto da cui l'antenna irraggia il segnale).

Domanda Cos' è un'antenna Direttiva(con un certo guadagno)?

Risposta Il guadagno di un'antenna è definito come il rapporto fra la potenza irradiata dall'antenna in esame nella direzione di massima direttività e la potenza
che irradierebbe un'antenna isotropa alimentata con la stessa

	potenza.

Domanda	Cos' è il dBi?
Risposta	Il guadagno di un'antenna è definito come il rapporto fra la densità di potenza irradiata dall'antenna in esame nella direzione di massima direttività (P 2) e la densità di potenza che irradierebbe un'antenna isotropa alimentata con la stessa potenza. Definiamo il dBi=10 log 10 (P 2 / P isotropica), dBm=10 log 10 (Potenza/ 1mW)

Domanda	Confronto fra Antenne direttive ed isotropiche
Risposta	In tabella è possibile osservare i vantaggi e gli svantaggi di ciascun tipo di antenna:

Tipologia	**Caratteristiche**	**Copertura**	**Installazione**
Isotrope	Coprono un angolo di 360°	Copertura relativamente bassa	Facili da installare
Direttive	Proiettano un cono relativamente ristretto	Copertura anche molto elevata	Richiedono un'attenta installazione

Domanda	La Legge
Risposta	L'EIRP è la Potenza Isotropica Effettiva Irradiata (Isotropica significa 'in ogni direzione') ed indica essenzialmente la potenza che effettivamente 'esce' dall'antenna. L'EIRP è sempre limitato per legge ed in Italia per i 2.4GHz questo limite è di 20dBm, pari a 100mW. Questo valore è la somma di: • potenza al connettore dell'Access Point/ Wireless Broadband Router • guadagno d'antenna espresso in dBi. La legge non fa distinzioni sul tipo di antenna utilizzato Questa potenza è la somma della potenza irradiabile e del guadagno dell'antenna Quindi per le antenne direttive la misurazione va effettuata nel cono di maggior irradiazione

	E' possibile accedere al sito del ministero delle comunicazioni (www.comunicazioni.it) per scaricare la modulistica e l'intera legge.

Domanda	Attenuazione di Spazio Libero?
Risposta	E' possibile utilizzare la formula di Friis per avere (in dB) l'attenuazione di spazio libero: $Attenuazione(dB)=92,45+20*Log_{10}F+20Log_{10}D$ D=espressa in Km F=frequenza in GHz Per avere un'idea nella tabella sottostante sono stati inserite le distanze più comuni (F=2.450GHz):

Distanza	Attenuazione in dB
100m	80,2
150m	83,7
200m	86,2
250m	88,2
300m	89,7
500m	94,2
750m	97,7
1000m	100,2
1500m	103,7
2000m	106,3

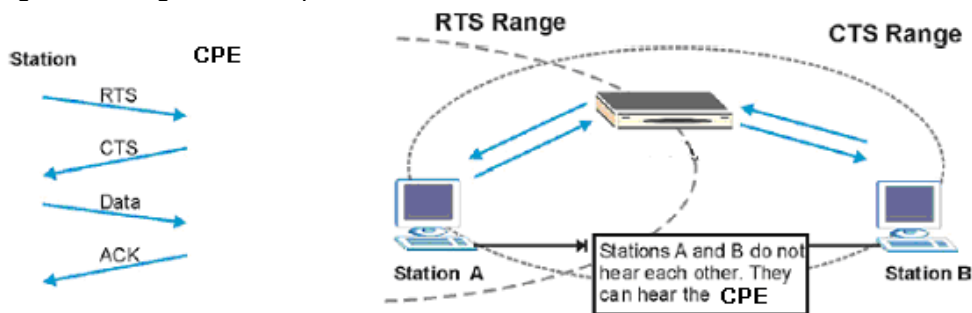
Partendo dal calcolo dell'attenuazione per una certa distanza è possibile utilizzare (per evitare calcoli) i seguenti accorgimenti:

- Si ricorda che al raddoppio della distanza è necessario aggiungere 6dB all'attenuazione.
- Si ricorda che quando si dimezza la distanza è necessario sottrarre 6dB all'attenuazione.

APPENDICE B:Come Avviene la comunicazione Wireless

La comunicazione in una WLAN avviene tramite onde radio che hanno una frequenza compresa tra 2.4Ghz e 2.48Ghz. Vengono dunque utilizzati circa 80Mhz di banda ISM (è una banda libera per applicazioni industriali, scientifiche e mediche).
La trasmissione avviene dunque utilizzando un mezzo condiviso e possono pertanto sorgere delle collisioni durante l'accesso da parte dei client wireless.
Il protocollo CSMA/CA ("carrier sense multiple access with collision avoidance") è responsabile di garantire una politica di accesso corretta al mezzo, limitando al massimo il numero di collisioni.
Un client(o nodo), infatti, prima di inviare un pacchetto dati si mette in ascolto e, rilevato il canale libero, invia i dati.

RTS/CTS

Quando due stazioni Wireless sono all'interno del range dello stesso Wireless Broadband Router ma non si vedono direttamente si ha un "nodo nascosto". La figura che segue illustra questa situazione.

La stazione A invia dei dati all'AP ma nel mentre non sa se la stazione B sta già utilizzando il canale. Se le due stazioni trasmettessero richieste di inizio trasmissione allo stesso tempo si avrebbero delle collisioni quando le informazioni giungono al Wireless Broadband Router.
Il protocollo RTS/CTS (Request To Send/Clear to Send) è stato disegnato per prevenire le collisioni quando si verificano situazioni di "nodi nascosti". Un RTS/CTS definisce la dimensione massima del frame di dati che è possibile trasmettere prima che la prossima richiesta RTS/CTS sia inoltrata. Quando un frame di dati supera il valore di RTS/CTS impostato (tra 0 e 2432 bytes), la stazione che vuole trasmettere deve inviare un messaggio RTS al Wireless

Broadband Router per ottenere il permesso ad iniziare. Il Wireless Broadband Router invia quindi a tutte le altre stazioni della rete Wireless un messaggio CTS vietando loro la trasmissione di dati.
A questo punto, il nodo ricevente, dopo aver controllato l'integrità dei dati ricevuti (a tal fine viene utilizzato una sorta di CRC) invia un messaggio di ACK per informare il trasmittente dell'avvenuta corretta ricezione del pacchetto.

L'utilizzo di questo protocollo unito all'invio di ACK (segnalazione di corretta ricezione di un frame) di corretta ricezione ed al traffico di gestione e controllo comporta un importante overhead che riduce, in maniera sensibile, il throughput massimo ottenibile.

Canali

Il range di frequenze radio usate dalle apparecchiature Wireless IEEE 802.11b/g è suddiviso in "canali"; la stessa cosa vale anche per dispositivi basati su specifiche 802.11n.
Il numero di canali disponibili dipende dall' area geografica di appartenenza. E' possibile selezionare canali differenti in modo da eliminare eventuali interferenze con gli Access Point/ Wireless Broadband Router vicini.
L'interferenza si verifica quando due o più canali si sovrappongono degradando le prestazioni, questa sovrapposizione è chiamata "Overlap".
E' consigliabile mantenere una distanza di 5 canali tra due utilizzati (es. AP1-canale 1, AP2-canale 6).

Modalità Operative

Lo standard integra 2 differenti modalità operative:

- Infrastructure: in questa modalità i differenti client si contendono il mezzo radio e quindi ai servizi messi a disposizione dalla rete. La gestione delle contese è affidata ad un'entità centralizzata che prende il nome di Punto d'Accesso. Con l'uso di algoritmi di sicurezza l'AP può anche essere responsabile dell'autenticazione dei client e cifratura del traffico.
- Ad Hoc: in questa modalità non è presente un AP ma soltanto una moltitudine di client che devono essere configurati con lo stesso SSID, lo stesso canale, in modalità Ad-Hoc e con la stessa chiave WEP.

APPENDICE C: Sicurezza nel Wireless

Per la natura stessa delle reti wireless tutta una nuova serie di considerazioni sulla sicurezza vanno affrontate. Il segnale radio può infatti essere intercettato da terzi non autorizzati che potrebbero cercare di estrarne informazioni preziose.
Sino ad oggi la sicurezza nelle reti WLAN è stata garantita dal protocollo WEP(Wired Equivalent Privacy) a 64/128. Purtroppo:

- le vulnerabilità WEP protocollo e la non facilità del contenimento del segnale wireless
- disattese aspettative di throughput

hanno generato, in taluni utenti, una certa diffidenza nei confronti della Tecnologia Wireless.
Per cercare di colmare alle lacune della sicurezza Wireless la IEEE sta sviluppando un nuovo standard, chiamato IEEE802.11i, che permetterà di rendere le reti wireless finalmente affidabili.
In attesa delle ratifica di questo standard la Wi-Fi Alliance ha derivato dalla versione preliminare un insieme si specifiche che va sotto il nome di WPA (Wi-Fi Protected Access).

Come opera il WEP

Il segnale radio, come già evidenziato in precedenza, è di difficile contenimento è può pertanto essere intercettato da utenti non autorizzati (è sufficiente che abbiano un comune client wireless in standard IEEE802.11b/g).
Il protocollo WEP nasce per limitare questo fenomeno.
Nel dettaglio i servizi offerti dal WEP sono:

- autenticazione delle stazioni che accedono ai servizi di rete
- integrità dei dati trasmessi sul canale radio (nessuna cambiamento è possibile senza che il sistema non se ne accorga)
- riservatezza dei dati trasmessi sul canale radio (nessuno può comprendere l'informazione contenuta nei pacchetti che sono cifrati con l'algoritmo RC4)

Le principali critiche mosse al WEP sono le seguenti:

- Una sola chiave segreta è utilizzata per l'autenticazione (di fatto non si autentica un client, al massimo si sa che il client appartiene al gruppo di utenti autorizzati)
- Un client che conosce la chiave può intercettare tutto il traffico scambiato dagli altri client wireless.
- La chiave di autenticazione è statica ed è usata anche per la cifratura (un attaccante può cercare di entrare nel sistema decifrando il traffico dati che contiene questa chiave)

- Debolezza nel modo con cui il WEP costruisce la chiave di cifratura (diversa ogni trama) coi cui l'RC4 cifra il messaggio
- Debole contro attacchi di integrità o che sfruttano la mancanza di autenticazione di ogni messaggio

Come opera il WPA e WPA2 (in modalità PSK e 802.11x)

In attesa delle ratifica dello standard IEEE802.11i la Wi-Fi Alliance ha derivato dalla versione preliminare un insieme di specifiche che va sotto il nome di WPA (Wi-Fi Protected Access).
Le caratteristiche peculiari del WPA sono:

- Integrazione del TKIP (Temporal Key Integrity Protocol) per permettere il cambio della chiave e migliora il controllo di integrità dei pacchetti
- Meccanismo avanzato per gestire l'autenticazione e il controllo degli accessi ai servizi di rete in modo centralizzato (802.11x tramite EAP, l'uso di TLS è obbligatorio)
- La chiave di autenticazione è diversa da quella utilizzata per la cifratura (che grazie al TKIP cambia continuamente)
- Permette l'autenticazione direttamente sull'AP (WPA-PSK)

Approvato di recente dalla Wi-Fi Alliance, il nuovo standard WPA2 è l'evoluzione del primo WPA (Wi-Fi Protected Access) che è oggi supportato dalla maggior parte degli apparati compatibili IEEE802.11g.
Lo standard WPA, richiesto prepotentemente dal mercato per porre fine alla debolezza intrinseca del WEP, ha purtroppo tratto dall'802.11i solo una parte delle specifiche.
Il nuovo WPA2 invece abbracciando pienamente l'IEEE802.11i ha necessariamente introdotto il supporto per l'Advanced Encryption Standard (AES), protocollo di cifratura utilizzato già da tempo nelle VPN IPSec.
I dispositivi WPA2 saranno compatibili con quelli WPA che però dovranno essere riaggiornati tramite il rilascio di nuovi firmware e/o driver. Il problema risiede nella capacità di calcolo (richiesta dall'AES) che rischierebbe di essere praticamente troppo elevata per gli apparati oggi in commercio.

Ogni sistema di cifratura dati è basato su password.
Queste possono essere lunghe, nel caso del WPA in PSK, da 8 sino a 63 caratteri.
Più lunga è la password e meno ha senso compiuto (usare caratteri alfanumerici, numeri e punteggiatura di ogni genere) più questa risulterà sicura.

APPENDICE D: Access Point o Router

Modalità Access Point

In questa modalità il Router è collegato alla vostra LAN tramite una delle 4 porte Fast Ethernet (e la porta WAN è inutilizzata).
In questo caso è necessario collocare il Wireless Router sulla stessa classe degli apparati cui è collegato.

Modalità Router (Con NAT abilitato)

Quando si implementa il Nat si isola di fatto la propria Lan dalla porta WAN (e quello cui questa è collegata). La Lan locale, se privata, deve avere gli indirizzi IP appartenenti ai seguenti blocchi (riservati dall'ente IANA per reti private).

CLASSE	IP Partenza	IP Finale	Subnet Mask
A	10.0.0.0	10.255.255.255	255.0.0.0
B	172.16.0.0	172.31.255.255	255.255.0.0
C	192.168.0.0	192.168.255.255	255.255.255.0

E' chiaramente raccomandato scegliere gli indirizzi della Lan appartenenti alla tabella di sopra (per ulteriori informazioni fare riferimento all'RFC 1597). Scegliendo dei blocchi pubblici potrebbero sorgere problemi di mancata visibilità di taluni siti internet.
Scenari più comuni:

- PC con IP appartenenti ad una classe privata, il cui default gateway è il Router Wireless che fa NAT. Può essere attivo o meno il DHCP (il Router prenderà sull'interfaccia WAN un indirizzo IP statico o dinamico, a seconda della configurazione). Il collegamento con l'ISP può essere uno qualsiasi tra quelli supportati (il default gateway del Router ADSL sarà dato automaticamente come i DNS in caso di PPPoE e PPPoA, dovranno essere inseriti in caso di altri protocolli come RFC1483/1577). In questo caso dunque una possibile configurazione della LAN sarebbe la seguente:

Host	Indirizzo IP	Maschera	Gateway	DNS
Router Lan IP	192.168.1.1	255.255.255.0		
PC A	192.168.1.2	255.255.255.0	192.168.1.1	Forniti ISP

PC B	192.168.1.3	255.255.255.0	192.168.1.1	Forniti ISP
PC C	192.168.1.4	255.255.255.0	192.168.1.1	Forniti ISP
PC X	192.168.1.n	255.255.255.0	192.168.1.1	Forniti ISP

In questo caso si è scelto di mantenere la rete 192.168.1.x e l'indirizzo IP (per il Wireless Broadband Router) di default. E' possibile in questo caso abilitare il DHCP server del Router (per assegnare ulteriori indirizzi IP, magari a PC portatili) ma bisogna prestare attenzione nello scegliere un pool di indirizzi compatibile (in questo caso bisognerà settare come IP starting 192.168.1.n+1, dove n+1<254).
E' comunque possibile cambiare la rete, avendo l'accortezza di sceglierla tra quelle riservata dallo IANA a tale utilizzo.

- PC con IP appartenenti ad una classe pubblica, in questo caso tutti i PC della Lan sono raggiungibili da Internet e l'interfaccia Lan del Router ha anch'essa un indirizzo IP pubblico. Il default gateway dei PC è l'indirizzo IP della Lan del Router che avrà chiaramente il NAT disabilitato. L'interfaccia WAN del Router prenderà un IP che può essere pubblico o privato, l'ISP fornirà comunque l'indirizzo del default gateway del Wireless Broadband Router assieme alla subnet mask. Questo scenario è tipico, ma non esclusivo, con l'uso del protocollo RFC 1483 o RFC 1577. Come già accennato è possibile che l'ISP utilizzi una punto-punto composta da indirizzi IP che possono essere pubblici o privati.

APPENDICE E: Considerazioni sulla Salute

Quando un organismo è immerso in un campo elettromagnetico avviene un'interazione nota come "effetto biologico". Non bisogna necessariamente associare all'"effetto biologico" un danno. Il problema può sorgere quando tale effetto supera la capacità di compensazione dell'organismo.
E' opportuno considerare che il livello di emissioni di un dispositivo wireless conforme alle direttive stabilite dall'IEEE (Institute of Electrical and Electronic Engineers) è notevolmente inferiore all'emissione generata da dispositivi di uso comune.
Un comune terminale GSM emette infatti una potenza che può arrivare e superare i 600mw, mentre un apparato UMTS emette una potenza del 20% inferiore.
A titolo di confronto un apparato Wireless difficilmente supera, in condizione di uso normale, i 17 dBm (circa 50mW) essendo di fatto oltre un ordine di grandezza inferiore.
Già queste considerazioni puramente energetiche dovrebbero tranquillizzare circa ogni eventuale dubbio.
Va inoltre considerato che l'uso del cellulare avviene ad una distanza tipica di qualche centimetro e dunque, essendo l'antenna di tipo isotropica, metà della potenza trasmessa attraversa la testa dell'utilizzatore e crea un effetto "riscaldamento" avvertibile soprattutto nei tessuti superficiali.
Nel caso di un apparato wireless possono presentarsi 2 casi diversi:

- Antenna isotropica: va considerato l'angolo solido con cui questa viene vista (generalmente qualche grado)
- Antenna direttiva: emette potenza solo nella zona di direttività

In entrambi i casi l'energia che arriva all'utilizzatore va da una frazione di quella trasmessa (e non la metà come nel caso del cellulare) sino ad arrivare a zero nel caso di antenna direttiva.
In tabella un grafico comparativo di quanto sin qui detto:

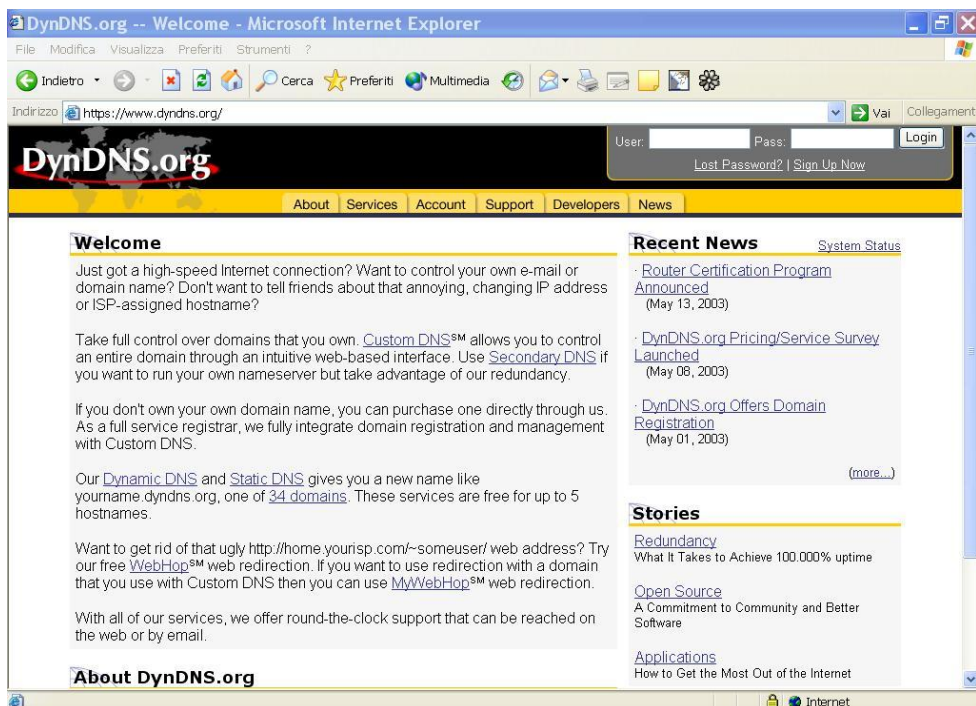
Apparato	Potenza Emessa	Angolo di Visuale	Potenza Effettiva
Wireless IEEE802.11b/g	**50mW**	1/15	<5mW
Cellulare GSM	**600mW**	1/2	Circa 300mW
Cellulare UMTS	**500mW**	1/2	Circa 250mW

Il Decreto del 20 Giugno 1995, n.458 (Legge Cautelativa dello Stato) impone di usare il telefonino tenendo l'antenna ad almeno 20cm da qualsiasi parte del proprio corpo.

Ad oggi, tutti gli studi effettuati hanno concluso che non esistono effetti termico-biologici pericolosi, a patto di rispettare le norme ETSI sull’emissione.

APPENDICE F: Regolamentazione

Taluni paesi europei utilizzano una legislazione differente sull'utilizzo delle frequenze ISM. Consultare la tabella sottostante per conoscere I canali utilizzabili.

Canali	Country
1-11	USA/CANADA
1-13	ETSI(Europe)
10-11	Spain
10-13	France
14	MKK
1-14	Japan (MKKI Telecom)
3-9	Israel
5-13	Israel

APPENDICE G: Dynamic DNS

Grazie all'adozione di questa features è possibile registrare un dominio pur se associato ad un IP dinamico. Ci sono una moltitudine di server DDNS che offrono gratuitamente questo tipo di servizio. E' sufficiente registrarsi per attivare in maniera gratuita ed immediata il servizio che consentirà di raggiungere (da remoto) sempre il Router ADSL2+. E' possibile in questo modo effettuare facilmente configurazioni da remoto, ospitare un sito WEB o FTP.
Ogni qual volta che l'Adsl2+ VPN Router si riconnetterà, tramite il client incorporato, comunicherà al server DDNS il nuovo indirizzo IP. In questo modo chiunque dall'esterno conoscendo l'URL conoscerà anche l'indirizzo IP che in quel momento è stato assegnato all'Adsl2+ VPN Router.
Vediamo, nel dettaglio come effettuare una registrazione con il gestore DDNS forse più famoso.

Andare nel sito:www.dyndns.org, cliccare su Account.

Effettuare la registrazione (cliccando su Create Account) inserendo:Username, Indirizzo Mail e Password.
Una mail di verifica registrazione sarà inviata all'indirizzo inserito. In questa mail sono contenute le istruzioni per proseguire la registrazione (è necessario confermare così il tutto entro 48 ore). Seguire le istruzioni contenute e compilare il form per terminare la fase di registrazione.
A questo punto tornare nel sito, andare su Services, evidenziare (nella parte sinistra) il menù Dynamic DNS e poi cliccare su Add Host.

Non resta che introdurre il Nome dell'host (evidenziare Enable WildCard) e scegliere il suffisso preferito e premere poi sul bottone Add Host per terminare.

APPENDICE H: WPS (Wi-Fi Protected Setup)

WPS (Wi-Fi Protected Setup) è un insieme di specifiche mirate a facilitare notevolmente le operazioni di aggiunta di dispositivi alla propria rete wireless e la messa in sicurezza della stessa con la sola pressione di un pulsante oppure tramite l'immissione di un codice PIN.
I dispositivi conformi alle specifiche WPS sono quindi in grado, in maniera molto semplice, di rilevare le reti con tale supporto, acquisirne le impostazioni basilari(quali SSID e canale) e negoziare in maniera del tutto automatica un profilo di sicurezza utiizzando i più avanzati algoritmi di crittografia come WPA e WPA2.
Nella configurazione PIN, un codice PIN univoco viene assegnato ad ogni dispositivo che deve far parte della rete; un adesivo o un etichetta posta sulla parte posteriore del client identificheranno tale codice in caso di PIN statico, o in alternativa questo verrà generato in maniera dinamica e visualizzato tramite utility.
Questo codice viene utilizzato per assicurare l'identificazione univoca della periferica e per evitare intrusioni all'interno della rete da parte di periferiche esterne. Gli utenti, per poter aggiungere il dispositivo alla rete, dovranno inserire all'interno del Registar (presente all'interno dell'Access Point), il codice PIN identificativo della periferica da connettere.
Nella configurazione PCB, l'utente sarà in grado di aggiungere periferiche e mettere in sicurezza la propria rete tramite la semplice pressione di un pulsante (fisico sugli Access Point e virtuale sui dispositivi client).
Di seguito una tabella riassuntiva sui vantaggi del supporto WPS e sulle modalità di configurazione:

Senza WPS	**Con WPS (PIN mode)**	**Con WPS (PCB mode)**
Accensione dell'Acces Point	Accensione dell'Acces Point	Accensione dell'Acces Point
Accesso all'Access Point	Attivazione del client	Attivazione del client
Configurazione dell'SSID	Generazione in maniera automatica dell'SSID e broadcasting della stessa.	Generazione in maniera automatica dell'SSID e broadcasting della stessa.
Attivazione della sicurezza	Accesso al Registar presente sull'Access Point	Pressione del bottone sull'Access Point e sul client
Impostazione della parola di accesso (WPA)	Insierimento del PIN relativo al client da	

o delle chiavi di accesso (WEP)	aggiungere.	
Attivazione del client	Avvio della sincronizzazione tra AP e client	
Selezione della rete a cui connettersi		
Inserimento della chiave di sicurezza per la connessione del client		

APPENDICE I: Caratteristiche Tecniche

STANDARDS	IEEE 802.3u 100BASE-TX Fast Ethernet IEEE 802.11g; IEEE 802.11b
PROTOCOL	CSMA/CD with ACK
RADIO TECHNOLOGY	DSSS/OFDM
DATA TRANSFER RATE	802.11n mode: up to 300Mbps (auto sense) 802.11g mode: up to 54Mbps (auto sense) 802.11b mode: up to 11Mbps (auto sense) Ethernet: 10Mbps (half duplex), 20Mbps (full-duplex) Fast Ethernet: 100Mbps (half duplex), 200Mbps (full- duplex)
RECEIVER SENSITIVITY	802.11n: -62dBm typical @ 300Mbps 802.11g: -68dBm typical @ 54Mbps 802.11b: -85dBm typical @ 11Mbps
TX POWER	802.11n: 14dBm typical 802.11g: 15dBm typical 802.11b: 18dBm typical
NETWORK CABLES	10BASE-T: 2-pair UTP Cat. 3,4,5 (100 m), EIA/TIA-568 100-ohm STP (100 m) 100BASE-TX: 2-pair UTP Cat. 5 (100 m), EIA/TIA-568 100-ohm STP (100 m)
FREQUENCY RANGE	2412 ~ 2484 MHz ISM band (channels 1 ~ 14)
MODULATION SCHEMES	DBPSK/DQPSK/CCK/OFDM
SECURITY	64/128-bits WEP Encryption; WPA, WPA-PSK,WPA2. WPA2-PSK
CHANNELS	1 ~ 11 channels (FCC); 1 ~ 13 channels (ETSI); 1 ~ 14 channels (MKK)
NUMBER OF PORTS	LAN: 4 x 10/100Mbps Auto-MDIX Fast Ethernet port WAN: 1 x 10/100Mbps Auto-MDIX Fast Ethernet port
DC INPUTS	DC 5V / 2.5A
POWER CONSUMPTION	7 W (Max)
TEMPERATURE	Operating: 0° ~ 40° C, Storage: -10° ~ 70° C
HUMIDITY	Operating: 10% ~ 90%, Storage: 5% ~ 90%
DIMENSIONS	147 x 115 x 35 mm (W x H x D) without Antenna
EMI	FCC Class B, CE Mark B

APPENDICE J: Supporto Offerto

Per qualunque altro problema o dubbio sul funzionamento del prodotto, è possibile contattare il servizio di assistenza tecnica Atlantis Land tramite l'apertura di un ticket on-line sul portale http://supporto.atlantis-land.com.

Nel caso non fosse possibile l'accesso al portale di supporto, è altresì possibile richiedere assistenza telefonica al numero 02/00632345.

Per esporre eventuali richieste di supporto prevendita o richieste di contatto , vi invitiamo ad utilizzare gli indirizzi mail info@atlantis-land.com oppure prevendite@atlantis-land.com.

Atlantis
Via Pelizza da Volpedo, 59
20092 Cinisello Balsamo (MI) Italy

Tel: +39.(0)2.93906085
Fax: +39.(0)2.66016.666
Help Desk :+39.(0)2.93907634
Email: info@atlantis-land.com
WWW: www.atlantis-land.com